

# POLÍTICA DE INTELIGENCIA ARTIFICIAL CEMENTOS ARGOS

CONTENIDO

1	Objetivo
2	Glosario
3	Alcance
4	Política
5	Gobierno
6	Anexos y Referencias
7	Periodicidad de revisión de la política
8	Aprobación

### 1. OBJETIVO

Establecer los marcos y directrices para el desarrollo, implementación y uso ético y seguro de la inteligencia artificial, en adelante IA. Esta política orientará el comportamiento de los colaboradores y terceros en relación con los sistemas de IA, garantizando el cumplimiento de leyes y regulaciones, la transparencia, la mitigación de riesgos y sesgos, y la protección de datos personales. A través de esta política, se proporcionarán guías claras para la adopción de medidas técnicas y organizacionales que aseguren la ciberseguridad y la integridad de los procesos impulsados por IA.

**Comentado [MML1]:** Tener en cuenta que todo lo aquí consagrado tiene que estar alineado con la ley y jurisdicción local con las que operamos

### 2. GLOSARIO

**Inteligencia Artificial (IA):** La inteligencia artificial se refiere a la simulación de procesos de inteligencia humana por parte de sistemas informáticos. Estos procesos incluyen el aprendizaje (la adquisición de información y reglas para usarla), el razonamiento (usar las reglas para alcanzar conclusiones aproximadas o definitivas) y la autocorrección.

**Sistemas de IA:** Un sistema de IA es cualquier sistema que utiliza técnicas de inteligencia artificial para realizar tareas que normalmente requieren inteligencia humana, como el reconocimiento de voz, la toma de decisiones, la traducción de idiomas y la percepción visual. Estos sistemas pueden ser software, hardware o una combinación de ambos.

**Tecnología de IA:** La tecnología de IA abarca las herramientas, técnicas y metodologías utilizadas para desarrollar y operar sistemas de inteligencia artificial. Esto incluye algoritmos de aprendizaje automático, redes neuronales, procesamiento del lenguaje natural y visión por computadora, entre otras.

**Aplicación de IA:** Una aplicación de IA es un uso específico de la tecnología de inteligencia artificial para resolver problemas o mejorar procesos en diversas áreas, como la salud, la educación, la manufactura, el comercio, la seguridad y muchos otros campos. Ejemplos incluyen asistentes virtuales, sistemas de recomendación y análisis predictivo.

**Sesgo de datos:** El sesgo de datos ocurre cuando los datos utilizados para entrenar un modelo de IA no representan adecuadamente la población o el fenómeno que se pretende analizar. Esto puede resultar en modelos que producen resultados injustos o imprecisos, favoreciendo o perjudicando inadvertidamente a ciertos grupos. La causa del sesgo puede estar en la recolección, el muestreo, la anotación o el procesamiento de los datos.

## Política de Inteligencia Artificial

Versión Inicial

**Algoritmo:** Un algoritmo es una secuencia finita de pasos o instrucciones que se siguen para resolver un problema o realizar una tarea específica. En el contexto de la IA, los algoritmos son fundamentales para el desarrollo de modelos de aprendizaje automático y otras aplicaciones de inteligencia artificial.

**Aprendizaje Automático (Machine Learning):** El aprendizaje automático es una rama de la inteligencia artificial que se centra en el desarrollo de algoritmos y técnicas que permiten a las computadoras aprender y mejorar automáticamente a partir de la experiencia sin ser explícitamente programadas para cada tarea. Esto se logra mediante el análisis de grandes cantidades de datos y la identificación de patrones.

**Redes Neuronales:** Las redes neuronales son un tipo de algoritmo de aprendizaje automático inspirado en el funcionamiento del cerebro humano. Consisten en capas de nodos (o "neuronas") que procesan información y pueden aprender a realizar tareas complejas mediante el ajuste de las conexiones entre nodos en respuesta a los datos de entrada.

**Procesamiento del Lenguaje Natural (NLP):** El procesamiento del lenguaje natural es una subdisciplina de la inteligencia artificial que se ocupa de la interacción entre las computadoras y los humanos mediante el lenguaje natural. El objetivo del NLP es permitir que las máquinas comprendan, interpreten y respondan a las entradas de lenguaje humano de manera útil y significativa.

**Ética de la IA:** La ética de la IA se refiere a los principios y directrices que deben seguirse en el desarrollo y la implementación de tecnologías de inteligencia artificial para asegurar que sean justas, transparentes y beneficien a la sociedad. Esto incluye consideraciones sobre la privacidad, la equidad, la responsabilidad y la mitigación de sesgos.

### 3. ALCANCE

Esta política de inteligencia artificial es de aplicación para todas las áreas de Cementos Argos S.A. y sus compañías filiales, incluyendo, el desarrollo de nuevos sistemas o aplicaciones de IA, la implementación de sistemas de IA existentes, la actualización o modificación de sistemas de IA en uso, y cualquier otro proceso que involucre el uso, aplicación o integración de tecnologías con inteligencia artificial.

Asimismo, esta política debe ser acogida por todos colaboradores, así como por todas las personas o entidades que desarrollan, implementan, utilizan o se relacionan con los sistemas de inteligencia artificial en las compañías.

### 4. POLÍTICA

#### POLÍTICA DE INTELIGENCIA ARTIFICIAL

Cementos Argos S.A. y sus compañías filiales, en cumplimiento de las leyes y regulaciones aplicables, se comprometen a utilizar la Inteligencia Artificial (IA) de manera responsable y ética, buscando obtener beneficios operativos y de negocio, al tiempo que protege los derechos y la seguridad de sus empleados, clientes y demás partes interesadas.

Mediante la implementación de prácticas de gobernanza y gestión de riesgos de IA, Cementos Argos S.A. y sus compañías filiales identificarán, evaluarán y mitigarán los posibles impactos adversos en áreas como la privacidad, la equidad, la transparencia y la rendición de cuentas. Asimismo, el grupo empresarial asegurará que el desarrollo y uso de sistemas de IA esté alineado con los principios éticos y de derechos humanos establecidos en las políticas y lineamientos enmarcadas en el gobierno corporativo de las compañías.

Frente al uso de la Inteligencia Artificial, las compañías, sus colaboradores y terceros se comprometen a:

- Establecer un marco de gobernanza y responsabilidad claro para el desarrollo, implementación y uso de sistemas de IA, el cual debe considerar las mejores prácticas en la materia y deberá ser actualizado periódicamente de acuerdo con la evolución de las tecnologías, de los riesgos relacionados y de las regulaciones aplicables. Para ello, se creará un comité de IA responsable con intervención de los equipos del Laboratorio DnA, TI Corporativo, Auditoría Interna, Legal Corporativa, Personas Corporativa y Seguridad Summa
- Promover el uso responsable de las tecnologías de inteligencia artificial, asegurando su implementación con medidas de seguridad adecuadas para proteger la confidencialidad, integridad y disponibilidad de los datos.
- Fomentar una cultura organizacional que promueva el uso confiable y benéfico de la IA, brindando capacitación y recursos a sus colaboradores por parte del Laboratorio DnA y equipos de Recursos Humanos de las regiones y el Corporativo de Cementos Argos.
- Adoptar medidas técnicas y organizacionales para garantizar la protección de los datos personales procesados por los sistemas de IA, respetando el derecho a la privacidad de los individuos, incluyendo medidas estrictas para prevenir la fuga de información en aplicaciones de inteligencia artificial, garantizando que los datos sensibles y confidenciales no sean expuestos o utilizados inapropiadamente.
- Desarrollar y utilizar todos los sistemas de IA de acuerdo con las leyes y regulaciones aplicables sobre protección de datos y privacidad, garantizando la transparencia sobre el uso de IA en los procesos de negocio.

## Política de Inteligencia Artificial

Versión Inicial

- Realizar evaluaciones exhaustivas de impacto de los sistemas de IA para identificar y mitigar potenciales riesgos, daños y sesgos en los datos, algoritmos y resultados, con el fin de evitar discriminación y tratamiento injusto.
- Identificar y clasificar los sistemas de IA de alto riesgo utilizados en la organización (por ejemplo, en áreas críticas como infraestructuras, procesos judiciales, etc.) y cumplir con las obligaciones establecidas para estos sistemas, como evaluación de riesgos, registro de uso, supervisión humana, etc.
- Implementar mecanismos de transparencia que permitan a los usuarios identificar claramente cuando están interactuando con o tomando decisiones sobre contenido generado por sistemas de IA, estableciendo procesos para etiquetar claramente textos, imágenes, audios, videos y comunicaciones generados y/o manipulados por sistemas de IA.
- Prohibir el uso de aplicaciones de IA que atenten contra los derechos fundamentales de los usuarios, como sistemas de categorización biométrica basados en características sensibles, reconocimiento facial masivo, sistemas de puntuación ciudadana, etc.
- Colaborar con las autoridades y partes interesadas relevantes para avanzar en el establecimiento de mejores prácticas y marcos regulatorios en torno a la Inteligencia Artificial.

## 5. GOBIERNO DE LA IA

Cementos Argos S.A. y sus compañías filiales definen la siguiente estructura organizacional con instancias, roles y responsabilidades, con el fin de asegurar un adecuado cumplimiento de la política de Inteligencia Artificial.

### Comité de ética y gobernanza de IA

- Revisar, aprobar, y monitorear el uso de IA
- Definir las responsabilidades y roles de los diferentes departamentos y equipos involucrados en el ciclo de vida de los sistemas de IA (por ejemplo, Laboratorio DnA, TI, Legal, Recursos Humanos, Ética/Cumplimiento).
- Definir un proceso periódico de revisión y actualización de esta política, considerando los cambios normativos, tecnológicos y de mejores prácticas en el campo de la IA.
- Detallar las medidas que se tomarán en caso de incumplimiento de los lineamientos establecidos en esta política.
- Establecer las consecuencias y sanciones disciplinarias aplicables a infracciones graves.

**Oficial de Gobierno de IA:** responsable de supervisar la implementación y el cumplimiento de la política de IA.

**Usuarios:** cualquier colaborador, proveedor, contratista, u otro tercero autorizado que utilice la información de las compañías en la ejecución de las actividades de su trabajo diario

### 6. RESPONSABILIDADES DE LOS USUARIOS

Como usuarios de modelos de inteligencia artificial, hay varias responsabilidades clave que los colaboradores y terceros de Cementos Argos y sus compañías filiales deberán adoptar para garantizar un uso ético y efectivo de estas herramientas. Entre las más importantes, se destacan las siguientes:

- Los modelos de IA están en constante desarrollo, ningún modelo es perfecto, y los resultados pueden estar sesgados o ser incorrectos. Por esta razón, un usuario de estas herramientas debe estar en capacidad de interpretar y validar las salidas o resultados de las solicitudes realizadas. Se recomienda aplicar metodologías de validación cruzada y corroboración con fuentes confiables antes de basar decisiones críticas en los resultados generados por IA.
- Los colaboradores deben evaluar el impacto de las decisiones automatizadas generadas por IA en los procesos de Cementos Argos, asegurándose de que los resultados no perjudiquen injustamente a clientes, empleados o terceros, y aplicando un juicio humano en situaciones crítica.
- Es responsabilidad de los colaboradores y terceros utilizar los modelos de IA de manera ética. Esto incluye respetar la privacidad y los datos personales, evitar el uso de la IA para propósitos maliciosos, y estar consciente de los posibles impactos sociales y laborales del uso de la IA. El uso indebido de la IA en tareas como generación de desinformación, deepfakes o manipulación de datos está estrictamente prohibido y será sancionado conforme a las políticas de seguridad de la información y cumplimiento normativo del Grupo Empresarial.
- Los modelos de IA pueden perpetuar o amplificar sesgos si no se manejan adecuadamente. Como usuario, se debe ser proactivo en identificar y mitigar esta brecha de acceso a la información.
- La IA es un campo en constante evolución, por lo que es crucial mantenerse al día con los avances y actualizaciones. Esto incluye aprender sobre nuevos modelos, metodologías, y también sobre cambios en la legislación y regulaciones relacionadas con la IA.
- Todos los colaboradores deben estar dispuestos a participar activamente en los entrenamientos y capacitaciones sobre el uso seguro y ético de la inteligencia artificial que sean indicados. La falta de participación en estos entrenamientos puede derivar en restricciones de acceso a herramientas de IA.
- En ninguna circunstancia, los colaboradores deben cargar, compartir o introducir información confidencial o documentos de uso interno o core de los negocios en plataformas de inteligencia artificial si estos quedan en la

base de conocimiento o expuestas al público, ya sea generativa o de otro tipo, que no estén autorizadas por el Grupo Empresarial.

- Se debe implementar Data Loss Prevention (DLP) y mecanismos de clasificación de información para mitigar el riesgo de fuga de datos a modelos de IA públicos. Además, cualquier solicitud de uso de IA en procesos críticos debe pasar por una evaluación de riesgos de ciberseguridad y cumplimiento normativo antes de su aprobación. El incumplimiento de este lineamiento puede comprometer la seguridad y confidencialidad de los datos corporativos.

### 7. USO Y MEDIDAS DE SEGURIDAD EN MODELOS DE IA PARA AREAS DE TECNOLOGIA, ARQUITECTURA Y DESARROLLO

Las áreas de Tecnología, Desarrollo, Arquitectura Tecnológica usuarias de modelos de IA dentro del Grupo Empresarial deben garantizar que el uso de estas herramientas se realice bajo estrictos controles de seguridad y cumplimiento normativo. Para ello, se establecen los siguientes lineamientos:

- Protección de datos y seguridad de la información:
  - Se debe garantizar que los datos utilizados para entrenar, evaluar o inferir con modelos de IA estén protegidos contra accesos no autorizados, aplicando controles de acceso basados en roles (RBAC) y políticas de menor privilegio.
  - Los datos utilizados en modelos de IA deben contar con la debida autorización y que se respetarán las restricciones impuestas por terceros sobre el uso de su información en IA.
  - Se prohíbe estrictamente el uso de modelos de IA en entornos de red pública no securizados o sin autenticación fuerte (MFA).
  - Para la protección de datos sensibles, se recomienda el uso de técnicas avanzadas de seguridad como cifrado homomórfico, privacidad diferencial y anonimización de datos antes de su procesamiento en modelos de IA.
- Ética y mitigación de sesgos en IA:
  - Se recomienda la implementación de técnicas de fairness-aware learning y debiasing en modelos entrenados internamente para reducir impactos discriminatorios en los resultados.

## Política de Inteligencia Artificial

Versión Inicial

- Todos los modelos de IA deben someterse a revisiones periódicas para identificar y mitigar sesgos, asegurando su alineación con principios de equidad, inclusión y no discriminación.
- En modelos generativos o de procesamiento de lenguaje natural (LLM), se debe validar la ausencia de sesgos perjudiciales que puedan afectar la reputación o generar decisiones erróneas.
- Desarrollo seguro de IA:
  - Se deben aplicar prácticas de DevSecOps en el desarrollo de modelos de IA, asegurando la seguridad desde la fase de diseño hasta el despliegue y monitoreo continuo.
  - Los modelos deben estar protegidos contra ataques adversariales, como model inversion attacks, data poisoning y prompt injection, mediante técnicas de robustez en modelos y monitoreo de inferencias maliciosas.
  - Se recomienda el uso de entornos Sandbox y segmentación de red para evitar riesgos de fuga de información al interactuar con modelos de IA.
- Gobernanza de IA y control de accesos:
  - La integración de IA en sistemas críticos debe pasar por un proceso de validación y pruebas de seguridad antes de su implementación en entornos de producción por el comité de gobierno de IA.

## 8. ANEXOS Y REFERENCIAS

- [Ley de Inteligencia Artificial – Regulación Unión Europea](#)
- Lineamientos de Inteligencia Artificial - Summa
- Anteproyecto para una Declaración de Derechos de la IA – Estados Unidos
- Políticas de Tratamiento de Datos Personales – Aplicables en los países de influencia del grupo [empresarial](#)
- Política Nacional para la Transformación Digital e Inteligencia Artificial (CONPES 3975) - Colombia
- Código de Conducta de las compañías del grupo empresarial - GRUPO ARGOS S.A. y sus compañías filiales (Cementos Argos, Celsia, Odinsa, Summa)

Comentado [MML2]: Solo la europea? Tener en cuenta la presencia de Argos en otros países(mensaje maria camila soto)

Comentado [MML3]: De que países?

## 9. PERIODICIDAD DE REVISIÓN DE LA POLÍTICA

Cada año o cada vez que se requiera.

## 10. APROBADO POR

- Instancia de aprobación: Comité de ética y gobernanza de IA – Juntas Directivas GRUPO ARGOS S.A. y sus compañías filiales (Cementos Argos, Celsia, Odinsa, Summa)

## CONTROL DE VERSIÓN

No. Rev.	Capítulo	Fecha	Autor	Descripción
V_001	Todos	Abril de 2024		Borrador - Emisión Inicial
V_002	Todos	Julio de 2024		Borrador – Compartido comités de Ciberseguridad
V_003	Todos	Mayo 2025		Integración de componentes de los lineamientos de Inteligencia Artificial de Summa