



POLÍTICA DE USO DE INTELIGENCIA ARTIFICIAL CORPORATIVA

POL-TI-005

Versión: 1.0
Fecha de emisión: 11 de abril de 2026
Área responsable: Departamento de Tecnología
Clasificación: Uso Interno
Próxima revisión: Abril 2027

AGROCOMMERCE S.A.

Santiago, Chile

ÍNDICE

1. OBJETIVO	3
1.1 Propósito General	3
1.2 Objetivos Específicos	3
2. ALCANCE	5
2.1 Alcance Personal	5
2.2 Alcance Tecnológico	5
2.3 Alcance Territorial y Temporal	6
3. PRINCIPIOS RECTORES	8
3.1 Principio de Responsabilidad	8
3.2 Principio de Transparencia	8
3.3 Principio de Confidencialidad	9
3.4 Principio de Verificación	9
3.5 Principio de Ética	9
4. HERRAMIENTAS AUTORIZADAS	11
4.1 Herramientas autorizadas	11
5. RESPONSABILIDADES	11
5.1 Responsabilidades de los Colaboradores	11
13. SANCIONES	12
13.1 Marco Sancionatorio	12
13.2. Clasificación de Faltas	12
13.3 Sanciones Aplicables	12
14. RIESGOS DE LA IA EN LA EMPRESA	13
15. REVISIÓN Y ACTUALIZACIÓN	15
Ciclo de Revisión	15
16. VIGENCIA	15
ANEXO A: APROBACIÓN Y FIRMAS	16
ANEXO B: HISTORIAL DE VERSIONES	17

1. OBJETIVO

1.1 Propósito General

La presente Política de Uso de Inteligencia Artificial Corporativa tiene como propósito fundamental establecer un marco normativo integral, claro y actualizado que regule todas las actividades relacionadas con el uso, implementación, desarrollo y gestión de herramientas basadas en Inteligencia Artificial dentro del grupo Agrocommerce. Este documento busca crear un equilibrio óptimo entre la adopción de tecnologías innovadoras que impulsen la competitividad empresarial y la protección de los activos de información, la privacidad de las personas y el cumplimiento de las obligaciones legales y éticas de la organización.

En el contexto actual de transformación digital acelerada, la Inteligencia Artificial representa una de las tecnologías más disruptivas y con mayor potencial para generar valor en las organizaciones. Sin embargo, su adopción sin un marco adecuado de gobernanza puede exponer a la empresa a riesgos significativos, incluyendo vulneraciones de seguridad, pérdida de información confidencial, incumplimientos normativos y daños reputacionales. Esta Política surge como respuesta a la necesidad de gestionar proactivamente estos riesgos mientras se aprovechan las oportunidades que ofrece la IA.

1.2 Objetivos Específicos

Los objetivos específicos que persigue esta Política son los siguientes:

a) Optimización de la Productividad

Establecer las condiciones y lineamientos que permitan a los colaboradores del grupo Agrocommerce utilizar herramientas de IA de manera efectiva para incrementar su productividad, automatizar tareas repetitivas, mejorar la calidad de sus entregables y liberar tiempo para actividades de mayor valor agregado. Se busca que la IA sea un multiplicador de capacidades que potencie el talento humano existente en la organización.

b) Protección de Activos de Información

Salvaguardar la información confidencial, los secretos comerciales, los datos de clientes y proveedores, la propiedad intelectual y todos los activos intangibles de la empresa frente a los riesgos inherentes al uso de herramientas de IA, particularmente aquellas basadas en servicios cloud o de terceros. Esto incluye establecer controles técnicos y procedimentales que prevengan la fuga o exposición inadvertida de información sensible.

c) Cumplimiento Normativo

Asegurar que el uso de IA en la organización cumpla con todas las disposiciones legales aplicables en Chile, incluyendo pero no limitándose a: la Ley N° 19.628 sobre Protección de la Vida Privada, la Ley N° 19.496 sobre Protección de los Derechos de los Consumidores, la Ley

N° 20.393 sobre Responsabilidad Penal de las Personas Jurídicas, el Código del Trabajo, y cualquier normativa sectorial aplicable al rubro agroindustrial y de comercio exterior.

d) Gestión de Riesgos

Identificar, evaluar y mitigar los riesgos asociados al uso de IA, incluyendo riesgos tecnológicos (fallas, vulnerabilidades, dependencia de proveedores), riesgos operacionales (errores en outputs, decisiones incorrectas basadas en IA), riesgos legales (responsabilidad por daños, infracciones de propiedad intelectual), riesgos éticos (sesgos algorítmicos, discriminación) y riesgos reputacionales (uso inapropiado, generación de contenido falso).

e) Fomento de la Innovación Responsable

Promover una cultura de innovación que aproveche las capacidades de la IA de manera responsable, ética y alineada con los valores corporativos del grupo Agrocommerce. Se busca que los colaboradores exploren nuevas formas de utilizar estas tecnologías para resolver problemas del negocio, siempre dentro del marco establecido por esta Política y con la debida supervisión humana.

f) Desarrollo de Capacidades

Establecer las bases para el desarrollo de capacidades internas en IA, incluyendo la formación de los colaboradores, la creación de conocimiento institucional sobre mejores prácticas, y la preparación de la organización para adoptar tecnologías de IA más avanzadas en el futuro, como agentes autónomos, sistemas de IA específicos del negocio y soluciones de IA generativa propietarias.

2. ALCANCE

2.1 Alcance Personal

Esta Política es de cumplimiento obligatorio para todas las personas que tengan relación laboral o contractual con el grupo Agrocommerce y que, en el ejercicio de sus funciones, utilicen, accedan, desarrollen o gestionen herramientas de Inteligencia Artificial. Específicamente, el alcance personal incluye:

a) Colaboradores Directos

- Todos los trabajadores con contrato de trabajo vigente, independientemente de su modalidad contractual (indefinido, plazo fijo, por obra o faena).
- Personal en período de prueba o inducción.
- Trabajadores en modalidad de teletrabajo o trabajo híbrido.
- Personal de todas las áreas funcionales: Administración, Finanzas, Comercial, Operaciones, Logística, Producción, Tecnología, Recursos Humanos, Legal, y cualquier otra.
- Colaboradores de todos los niveles jerárquicos, desde la alta dirección hasta el personal operativo.

b) Personal Externo

- Contratistas y subcontratistas que presten servicios en dependencias de la empresa o que accedan a sistemas de información del grupo Agrocommerce.
- Consultores externos en cualquier área (tecnología, gestión, legal, financiero, etc.).
- Auditores externos que requieran acceso a información de la empresa.
- Proveedores de servicios tecnológicos, incluyendo desarrolladores, integradores y personal de soporte.
- Practicantes, estudiantes en práctica profesional y personal en programas de formación.
- Cualquier tercero autorizado a acceder a los sistemas de información de la empresa.
- Este personal externo debe estar autorizado por la Gerencia del Grupo Agrocommerce.

2.2 Alcance Tecnológico

Esta Política aplica a todas las tecnologías, herramientas, plataformas, aplicaciones y sistemas que utilicen capacidades de Inteligencia Artificial en cualquiera de sus formas. El alcance tecnológico incluye, sin limitarse a:

a) Asistentes Conversacionales y Chatbots

- Modelos de Lenguaje Grande (LLMs) como Claude (Anthropic), ChatGPT (OpenAI), Gemini (Google), Copilot (Microsoft), Llama (Meta), y cualquier otro.

-
- Chatbots empresariales integrados en plataformas de atención al cliente o soporte interno.
 - Asistentes de voz y sistemas de procesamiento de lenguaje natural.

b) Herramientas de IA Generativa

- Generadores de imágenes como DALL-E, Midjourney, Stable Diffusion, Adobe Firefly.
- Generadores de video y animación con IA.
- Sintetizadores de voz y herramientas de clonación de audio.
- Generadores de música y efectos de sonido.
- Herramientas de generación de código y asistentes de programación como GitHub Copilot, Amazon CodeWhisperer, Cursor.

c) Herramientas de Análisis y Automatización

- Plataformas de análisis predictivo y machine learning.
- Herramientas de automatización robótica de procesos (RPA) con capacidades de IA.
- Sistemas de reconocimiento de patrones y detección de anomalías.
- Herramientas de análisis de sentimiento y procesamiento de texto.
- Sistemas de clasificación y categorización automática de documentos.

d) IA Integrada en Aplicaciones Empresariales

- Funcionalidades de IA en Microsoft 365 (Copilot en Word, Excel, PowerPoint, Outlook, Teams).
- Capacidades de IA en sistemas ERP, CRM y otras aplicaciones de negocio.
- Extensiones y plugins de IA para navegadores y aplicaciones de escritorio.
- APIs y servicios de IA consumidos por aplicaciones internas.

2.3 Alcance Territorial y Temporal

Esta Política aplica en todo el territorio donde el grupo Agrocommerce realice operaciones, incluyendo la casa matriz, sucursales, bodegas, centros de distribución y cualquier ubicación donde trabajen colaboradores de la empresa. Asimismo, aplica al uso de herramientas de IA:

- Dentro de las instalaciones de la empresa utilizando equipos corporativos.
- Fuera de las instalaciones en modalidad de teletrabajo o trabajo remoto.
- En dispositivos personales cuando se acceda a información o sistemas de la empresa (BYOD, bring your own device).
- Durante viajes de trabajo o en eventos corporativos.
- Las 24 horas del día, los 7 días de la semana, en cualquier momento en que se realicen actividades laborales.

3. PRINCIPIOS RECTORES

El uso de Inteligencia Artificial en el grupo Agrocommerce se fundamenta en los siguientes principios rectores, los cuales constituyen el marco ético y operacional que debe guiar todas las decisiones relacionadas con la adopción, uso y gestión de estas tecnologías:

3.1 Principio de Responsabilidad

Todo colaborador que utilice herramientas de IA es personalmente responsable del uso que haga de ellas y de los resultados que produzca con su asistencia. La IA es una herramienta de apoyo y potenciación de capacidades, pero nunca un sustituto del juicio profesional, el criterio experto o la responsabilidad individual.

Este principio implica que:

- El colaborador debe comprender las limitaciones de la herramienta de IA que utiliza y no confiar ciegamente en sus outputs.
- Los errores, omisiones o problemas derivados del uso de IA son responsabilidad del colaborador que la utilizó, no de la herramienta.
- No es aceptable justificar un error profesional argumentando que "lo hizo la IA" o que "la IA me dijo que era correcto".
- El colaborador debe mantener el nivel de diligencia profesional que se espera de su cargo, independientemente de si usa IA o no.
- **Las decisiones críticas siempre deben tener validación y aprobación humana, especialmente aquellas con impacto financiero, legal o en personas.**

3.2 Principio de Transparencia

El uso de IA debe ser transparente y comunicado cuando sea relevante para terceros o cuando la naturaleza de la tarea lo amerite. La transparencia genera confianza y permite que las partes interesadas comprendan cómo se llegó a determinados resultados o decisiones.

Aplicaciones prácticas de este principio:

- Si un documento, informe o análisis fue elaborado con asistencia significativa de IA, esto debe ser declarado cuando sea apropiado.
- En comunicaciones externas formales (contratos, propuestas comerciales, documentos legales), se debe indicar si hubo uso de IA en su elaboración cuando esto sea relevante para la contraparte.
- Los clientes, proveedores y socios comerciales deben ser informados cuando interactúen con sistemas automatizados de IA en nombre de la empresa.
- Internamente, los equipos deben compartir abiertamente las herramientas y técnicas de IA que utilizan para fomentar el aprendizaje colectivo.

- Los procesos de decisión que involucren IA deben ser documentados para permitir trazabilidad y auditoría.

3.3 Principio de Confidencialidad

La información confidencial del grupo Agrocommerce, sus clientes, proveedores y colaboradores debe ser protegida en todo momento durante el uso de herramientas de IA. Ninguna eficiencia o beneficio potencial justifica poner en riesgo la confidencialidad de la información.

Este principio establece que:

- La información clasificada como Confidencial o Estrictamente Confidencial no debe ser ingresada en herramientas de IA públicas o no autorizadas bajo ninguna circunstancia.
- Antes de usar información en una herramienta de IA, el colaborador debe evaluar su clasificación y los riesgos asociados.
- Los prompts deben ser diseñados de manera que no requieran revelar información sensible para obtener el resultado deseado.
- Se deben utilizar técnicas de anonimización cuando sea estrictamente necesario procesar información sensible.
- Los historiales de conversación con información sensible deben ser eliminados periódicamente.

3.4 Principio de Verificación

Todo resultado, contenido, dato, cifra, cita, referencia o información generada por una herramienta de IA debe ser verificada y validada por el usuario antes de su uso, difusión, implementación o toma de decisiones basada en ella. Este principio es crítico debido al fenómeno de las alucinaciones y las limitaciones inherentes de los modelos de IA.

La verificación debe incluir:

- Comprobación de la exactitud factual de datos, cifras, estadísticas y afirmaciones.
- Validación de citas, referencias bibliográficas, normativas o legales mencionadas.
- Revisión de la coherencia lógica y la razonabilidad de los argumentos.
- Confirmación de que el contenido es apropiado para el contexto y la audiencia objetivo.
- Verificación de que no existen sesgos, discriminación o contenido inapropiado.
- Aseguramiento de que el contenido no infringe derechos de propiedad intelectual de terceros.

3.5 Principio de Ética

El uso de IA en el grupo Agrocommerce debe ajustarse a los más altos estándares éticos, a los valores corporativos de la empresa y a las expectativas razonables de la sociedad sobre el uso responsable de estas tecnologías.

Implicaciones de este principio:

- Está prohibido utilizar IA para fines discriminatorios, ofensivos, difamatorios o que atenten contra la dignidad de las personas.
- No se debe utilizar IA para crear contenido falso, engañoso o manipulador que pueda dañar a terceros.
- El uso de IA no debe contribuir a perpetuar o amplificar sesgos sociales, de género, raciales o de cualquier otro tipo.
- Se debe respetar la autonomía y privacidad de las personas en cualquier aplicación de IA.
- El uso de IA debe contribuir al bienestar de los colaboradores, no a su reemplazo indiscriminado o precarización laboral.

4. HERRAMIENTAS AUTORIZADAS

4.1 Herramientas autorizadas

La Gerencia es responsable de mantener un catálogo actualizado de herramientas de IA autorizadas para uso corporativo. Este catálogo se publica en la Intranet corporativa y se actualiza cada vez que se aprueba o revoca la autorización de una herramienta

5. RESPONSABILIDADES

El cumplimiento efectivo de esta Política requiere la participación activa de todos los niveles de la organización. A continuación, se detallan las responsabilidades específicas de cada grupo:

5.1 Responsabilidades de los Colaboradores

Todo colaborador que utilice herramientas de IA en el ejercicio de sus funciones tiene las siguientes responsabilidades:

Conocimiento y Cumplimiento

- Leer, comprender y cumplir íntegramente esta Política y sus actualizaciones.
- Mantenerse informado sobre las herramientas autorizadas y sus condiciones de uso.
- Consultar a TI ante cualquier duda sobre la aplicación de esta Política.

Protección de Información

- Proteger la información confidencial de la empresa en todo momento.
- Gestionar adecuadamente los historiales de conversación.
- No compartir credenciales de acceso a herramientas de IA.

Reporte y Colaboración

- Reportar inmediatamente cualquier incidente de seguridad o uso indebido de IA.
- Compartir buenas prácticas y aprendizajes con el equipo.
- Proponer mejoras y nuevos usos de IA que aporten valor.
- Colaborar con las auditorías y revisiones de cumplimiento.

13. SANCIONES

13.1 Marco Sancionatorio

El incumplimiento de esta Política constituye una infracción a las obligaciones laborales del colaborador y puede dar lugar a la aplicación de medidas disciplinarias, conforme al Reglamento Interno de Orden, Higiene y Seguridad del grupo Agrocommerce y a la legislación laboral vigente.

13.2. Clasificación de Faltas

Las infracciones a esta Política se clasifican según su gravedad:

Faltas Leves

Se consideran faltas leves aquellas que no causan perjuicio significativo a la empresa ni a terceros, tales como:

- Omisión de verificación de outputs de IA en tareas de bajo impacto.
- Desconocimiento de esta Política.

Faltas Moderadas

Se consideran faltas moderadas aquellas que generan riesgo potencial o impacto limitado:

- Compartir información de Uso Interno en herramientas de IA sin las debidas precauciones.
- Reincidencia en faltas leves.
- No reporte de incidentes menores relacionados con IA.

Faltas Graves

Se consideran faltas graves aquellas que causan o pueden causar perjuicio significativo:

- Uso de herramientas de IA no autorizadas (Privadas o corporativa)
- Compartir información Confidencial o Estrictamente Confidencial en herramientas de IA no autorizadas.
- Procesar datos personales en herramientas de IA sin autorización.
- Generar contenido discriminatorio, ofensivo o dañino utilizando IA.
- Suplantar identidades o crear contenido fraudulento con IA.
- Eludir controles de seguridad utilizando IA.
- Ocultar o no reportar incidentes graves.
- Reincidencia en faltas moderadas.

13.3 Sanciones Aplicables

Gravedad	Sanciones Aplicables
LEVE	Amonestación verbal, capacitación obligatoria adicional, seguimiento
MODERADA	Amonestación escrita, restricción temporal de acceso a herramientas, capacitación obligatoria, registro en carpeta personal
GRAVE	Suspensión de funciones, restricción permanente de acceso, término de contrato según corresponda, acciones legales si procede

14. RIESGOS DE LA IA EN LA EMPRESA

El Uso e implantación de las IA involucran **tres categorías de riesgos críticos** en la organización:

gobernanza, cultura interna y reputación, destacando que estos riesgos **no son inmediatos**, sino que aparecen cuando la IA ya está integrada en los procesos.

14.1. Riesgos éticos y de gobernanza

Se relacionan con **cómo se toman decisiones dentro de la empresa**.

Principales riesgos:

- Sesgos en decisiones → resultados injustos pero con apariencia objetiva
- Falta de explicabilidad → imposibilidad de justificar decisiones
- Dilución de responsabilidad → nadie responde (“lo dijo la IA”)
- Uso indebido no evidente → manipulación o superficialidad en análisis

Idea clave:

La IA puede afectar directamente la calidad y legitimidad de las decisiones.

Controles propuestos:

- La IA **asiste, no decide**
- Responsabilidad humana definida
- Exigir explicaciones mínimas
- Auditoría en procesos críticos

14.2. Riesgos laborales y culturales

Impactan en **cómo trabajan y piensan las personas dentro de la empresa.**

Principales riesgos:

- Pérdida de criterio profesional (dependencia de IA)
- “Productividad falsa” (más volumen, menos valor real)
- Desalineación cultural (usuarios vs resistentes)
- Temor laboral y resistencia pasiva
- Uso oportunista (aparentar capacidades sin tenerlas)
-

Idea clave:

La IA puede aumentar velocidad, pero deteriorar la calidad si no se gestiona bien.

Controles propuestos:

- Capacitación en **criterio + uso de IA**
- Medir desempeño por impacto, no volumen
- Definir claramente cuándo usar IA y cuándo no

14.3. Riesgos reputacionales

Son los más visibles y de impacto inmediato hacia el exterior.

Principales riesgos:

- Errores frente a clientes (respuestas o propuestas incorrectas)
- Uso indebido o percepción de mal uso de datos
- Deshumanización del servicio
- Crisis por automatizaciones mal diseñadas
- Inconsistencia en comunicaciones

Idea clave:

Un solo error puede escalar rápidamente a crisis reputacional.

Controles propuestos:

- Supervisión estricta en contacto con clientes
- Revisión humana en comunicaciones críticas
- Protocolos de crisis
- Coherencia comunicacional centralizada

15. REVISIÓN Y ACTUALIZACIÓN

Ciclo de Revisión

Esta Política será revisada de manera ordinaria al menos una vez al año, o de manera extraordinaria cuando ocurran eventos que ameriten su actualización anticipada.

.

16. VIGENCIA

Esta Política de Uso de Inteligencia Artificial Corporativa entra en vigencia a partir del 11 de abril de 2026 y permanecerá en vigor hasta su derogación expresa o su reemplazo por una versión actualizada.

A partir de su entrada en vigencia, esta Política deroga cualquier instrucción, comunicación o lineamiento previo relacionado con el uso de herramientas de Inteligencia Artificial en la empresa que pudiera existir.

Todos los colaboradores activos a la fecha de vigencia deberán completar la capacitación obligatoria sobre esta Política dentro de los 30 días siguientes a su publicación.

ANEXO A: APROBACIÓN Y FIRMAS

Gerente de Tecnología
Elaborado por

Gerente General
Aprobado por

Gerente de Recursos Humanos
Revisado por

Asesor Legal
Revisado por

Fecha de aprobación: 11 de abril de 2026

ANEXO B: HISTORIAL DE VERSIONES

Versión	Fecha	Descripción del Cambio	Autor
1.0	11 de abril de 2026	Versión inicial del documento. Establece marco completo de gobernanza para uso de IA en la organización.	Gerencia de Tecnología