

ELABORADO POR:
Gerencia de Tecnología
de la Información

REVISADO POR:
Comité de Gerencia

APROBADO POR:
Gerencia General

Código: GIDI-P001
Versión: 01
Aprobado: 25 de Agosto 2026

POLÍTICA PARA EL USO RESPONSABLE DE INTELIGENCIA ARTIFICIAL

ACEROS AREQUIPA

1. OBJETIVO

Establecer los principios, responsabilidades y requisitos corporativos para la gobernanza y gestión de los sistemas de inteligencia artificial (IA) durante todo su ciclo de vida, asegurando que su utilización contribuya a los objetivos estratégicos y operativos de Corporación Aceros Arequipa S.A. y sus subsidiarias, de manera segura, responsable, ética, legal y proporcional al nivel de riesgo.

La presente Política busca proteger a las personas, la seguridad y confidencialidad de la información, los activos, los procesos, la continuidad operacional, la propiedad intelectual y la reputación de la Corporación, promoviendo al mismo tiempo la innovación y la generación de valor mediante el uso responsable de la inteligencia artificial.

2. ALCANCE

La presente Política es aplicable a los colaboradores, funcionarios, dueños de proceso, áreas usuarias, proveedores, contratistas y terceros que, en el marco de su relación con Corporación Aceros Arequipa S.A. y sus subsidiarias, participen en cualquier etapa del ciclo de vida de sistemas de inteligencia artificial, incluyendo su evaluación, aprobación, adquisición, diseño, desarrollo, implementación, integración, uso, administración, monitoreo, modificación y retiro.

Comprende las soluciones desarrolladas internamente o provistas por terceros, tales como sistemas de IA generativa, modelos predictivos, analítica avanzada, visión computacional, procesamiento de lenguaje, asistentes, agentes y otras aplicaciones de inteligencia artificial. También comprende las funcionalidades de IA incorporadas en plataformas, aplicaciones, servicios en la nube, equipos, maquinarias, sistemas de automatización y demás soluciones tecnológicas utilizadas por la Corporación.

3. MARCO NORMATIVO O DE REFERENCIA

La presente Política se aplica conforme con la normativa vigente relacionada con el uso responsable de la inteligencia artificial, la protección de datos personales, la seguridad de la información, la propiedad intelectual y los derechos de las personas y demás materias vinculadas al uso de tecnologías digitales, tomando como referencia, entre otras disposiciones aplicables, la Ley Nro. 31814, "Ley que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país", y su Reglamento, aprobado mediante D.S. Nro. 115-2025-PCM; así como la Ley Nro. 29733, "Ley de Protección de Datos Personales", y su Reglamento, aprobado mediante D.S. Nro. 016-2024-JUS, sin perjuicio de la aplicación de cualquier otra norma que resulte pertinente según la naturaleza de cada caso concreto.

Asimismo, se complementa con las políticas y lineamientos internos de la Corporación y con las buenas prácticas internacionales aplicables, de acuerdo con la naturaleza y el nivel de riesgo de cada caso de uso de inteligencia artificial.

4. DEFINICIONES

- **Inteligencia artificial:** Conjunto de tecnologías capaces de simular capacidades de la inteligencia humana para procesar información, aprender de datos, identificar patrones, generar contenido, realizar predicciones, formular recomendaciones, tomar decisiones o ejecutar acciones, con distintos niveles de autonomía y orientados al logro de objetivos definidos.

- **Inteligencia artificial generativa:** Tipo de inteligencia artificial capaz de generar contenido nuevo, como texto, imágenes, audio, video, código o análisis, a partir de instrucciones o datos proporcionados por el usuario.

- **Uso responsable de inteligencia artificial:** Aplicación de herramientas de inteligencia artificial bajo criterios de legalidad, ética, seguridad, privacidad, transparencia, supervisión humana, prevención de sesgos, proporcionalidad y adecuada gestión de riesgos.

- **Caso de uso de inteligencia artificial:** Aplicación específica de un sistema de inteligencia artificial dentro de un proceso o actividad de la Corporación, con una finalidad, alcance, responsables, usuarios y resultados esperados definidos.

- **Nivel de riesgo:** Grado de exposición o impacto potencial asociado con un sistema o caso de uso de inteligencia artificial, determinado de acuerdo con los criterios y la metodología de Gestión Integral de Riesgos (GIRO) establecida por la Corporación.

- **Supervisión humana:** Revisión, validación, intervención o escalamiento realizado por personas responsables, especialmente cuando los resultados generados por inteligencia artificial puedan influir en decisiones críticas, sensibles o de impacto relevante.

- **Sesgo algorítmico:** Resultado, recomendación o comportamiento de una herramienta de inteligencia artificial que pueda generar diferencias injustificadas, discriminatorias o no razonables entre personas, grupos de interés o situaciones comparables.

- **Soluciones de IA provistas por terceros:** Plataformas, modelos, aplicaciones, servicios en la nube, sistemas o funcionalidades de inteligencia artificial que son desarrollados, administrados o puestos a disposición por proveedores externos.

5. LINEAMIENTOS DE ACTUACIÓN

El uso de sistemas de inteligencia artificial en la Corporación deberá observar los siguientes criterios, aplicados de manera proporcional a la naturaleza, finalidad, alcance y nivel de riesgo de cada caso de uso:

5.1 Privacidad y protección de datos

Los sistemas de inteligencia artificial deberán utilizarse respetando la privacidad y la normativa de protección de datos personales. El ingreso, tratamiento o transferencia de datos personales, información confidencial, estratégica o restringida solo estará permitido cuando sea necesario, se encuentre autorizado y se realice mediante herramientas y controles aprobados por la Corporación.

5.2 Ciberseguridad y seguridad de la información

Los sistemas de inteligencia artificial deberán cumplir los controles corporativos de ciberseguridad y seguridad de la información, de acuerdo con la criticidad del proceso, la clasificación de la información y el nivel de riesgo del caso de uso, a fin de proteger la confidencialidad, integridad y disponibilidad de los datos, sistemas y operaciones de la Corporación.

5.3 Prevención de sesgos y trato justo

Los sistemas de inteligencia artificial deberán ser evaluados y supervisados, de manera periódica, para identificar, prevenir y mitigar sesgos, errores, resultados discriminatorios o injustificados que puedan afectar a colaboradores, clientes, proveedores, comunidades u otros grupos de interés, especialmente cuando sus resultados influyan en decisiones relevantes sobre personas.

5.4 Supervisión humana en decisiones críticas

Los sistemas de inteligencia artificial deberán utilizarse como herramientas de apoyo y no sustituirán la responsabilidad ni el criterio profesional de las personas. Las decisiones críticas o de impacto relevante deberán contar con mecanismos de revisión, validación, intervención y, cuando corresponda, aprobación humana.

5.5 Transparencia y explicabilidad

El uso de sistemas de inteligencia artificial deberá ser transparente y comprensible de acuerdo con su naturaleza y nivel de riesgo. La Corporación deberá contar con información suficiente sobre su finalidad, alcance, capacidades, limitaciones, criterios de uso y nivel de confiabilidad esperado.

5.6 Responsabilidad y rendición de cuentas

Todo sistema o caso de uso de inteligencia artificial deberá contar con responsables identificados para su aprobación, implementación, operación y supervisión. El uso de inteligencia artificial no exime a las personas, áreas o instancias correspondientes de sus responsabilidades funcionales, legales, éticas o corporativas.

5.7 Confiabilidad y límites de uso

Los sistemas de inteligencia artificial deberán utilizarse únicamente para las finalidades y dentro de los alcances autorizados. Sus resultados deberán ser revisados y validados antes de ser utilizados en decisiones, comunicaciones, documentos, operaciones o entregables de la Corporación, considerando sus limitaciones y el impacto potencial de errores o resultados inexactos.

5.8 Usos no permitidos

Queda prohibido utilizar sistemas de inteligencia artificial para fines ilícitos, discriminatorios o contrarios a los derechos fundamentales, así como para realizar actividades que impliquen manipulación indebida, explotación de vulnerabilidades, clasificación o perfilamiento injustificado de personas, vigilancia o identificación biométrica no autorizada, generación o difusión deliberada de información falsa, evasión de controles corporativos, infracción de derechos de propiedad intelectual o vulneración de la privacidad y la protección de datos personales.

Tampoco se podrá ingresar, registrar, cargar, compartir o procesar información de la Corporación en sistemas de inteligencia artificial no autorizados.

Las decisiones críticas no podrán adoptarse o ejecutarse exclusivamente mediante sistemas de inteligencia artificial y deberán contar con la intervención y supervisión humana correspondiente al nivel de riesgo del caso de uso.

6. RESPONSABILIDADES

Las Gerencias y Dueños de Proceso que adquieran, desarrollen, implementen o utilicen sistemas de inteligencia artificial serán responsables de definir su finalidad y alcance, identificar y evaluar los riesgos asociados, asegurar su uso conforme con la presente Política y mantener una supervisión humana efectiva y proporcional al nivel de riesgo sobre sus resultados. Asimismo, deberán implementar las medidas de control necesarias para prevenir, mitigar y gestionar los riesgos identificados durante su uso.

El área de Tecnología de la Información será responsable de establecer los lineamientos, estándares y arquitecturas tecnológicas aplicables al uso de inteligencia artificial, coordinar la evaluación y aprobación de las soluciones desde la perspectiva tecnológica, mantener el "Registro Corporativo de Sistemas y Casos de Uso de IA" y definir los controles tecnológicos y de seguridad aplicables, en coordinación con las Gerencias, Dueños de Proceso y demás áreas especializadas que correspondan, según la naturaleza, criticidad y nivel de riesgo de cada caso de uso.

Los usuarios deberán utilizar únicamente las herramientas de inteligencia artificial autorizadas por la empresa y de acuerdo con las condiciones establecidas para su uso. Asimismo, deberán proteger la información de la Corporación y los datos personales a los que tengan acceso, verificar la exactitud, pertinencia y confiabilidad de los resultados generados por la IA antes de utilizarlos, comunicarlos o difundirlos, y reportar oportunamente cualquier uso no autorizado, uso indebido, vulnerabilidad, incidente, resultado anómalo o riesgo identificado.

7. GESTIÓN DEL CICLO DE VIDA DE LOS SISTEMAS DE IA

Los sistemas y casos de uso de inteligencia artificial deberán ser registrados, clasificados según su nivel de riesgo, evaluados, aprobados, implementados, utilizados, monitoreados y retirados de manera controlada. Antes de su implementación, deberá verificarse su alineamiento con los objetivos de la Corporación, la normativa vigente y los controles internos aplicables. Durante su operación, las áreas responsables deberán supervisar su desempeño, validar sus resultados y gestionar oportunamente los riesgos, incidentes, cambios o desviaciones identificados.

Todo cambio relevante en su finalidad, alcance, datos utilizados, tecnología o proveedor deberá ser evaluado antes de su implementación y podrá requerir una nueva aprobación.

8. SOLUCIONES DE IA PROVISTAS POR TERCEROS

Cuando la empresa utilice herramientas, plataformas o servicios de inteligencia artificial provistos por terceros, el área usuaria, junto con el área de TI, deberá evaluar, de manera razonable y según el nivel de riesgo, aspectos relacionados con privacidad, seguridad de la información, condiciones de uso, confiabilidad, soporte, continuidad, tratamiento de datos, limitaciones de la herramienta y prácticas de uso responsable.

9. REPORTE Y GESTIÓN DE INCIDENTES DE IA

Los colaboradores y terceros deberán reportar oportunamente, mediante los canales establecidos por la Corporación, cualquier incidente, vulnerabilidad, uso no autorizado, resultado anómalo o situación de riesgo relacionada con sistemas de inteligencia artificial. Los reportes serán evaluados y gestionados por las áreas competentes según su naturaleza, impacto y nivel de riesgo, pudiendo suspenderse preventivamente el sistema o caso de uso cuando resulte necesario.

Las consultas sobre la aplicación de esta Política serán canalizadas al área de Tecnología de la Información o a las áreas específicas de acuerdo con cada caso de uso.

10. FORMACIÓN Y CONCIENTIZACIÓN EN INTELIGENCIA ARTIFICIAL

La Corporación promoverá la formación y concientización de los colaboradores que desarrollen, gestionen o utilicen sistemas de inteligencia artificial, de acuerdo con sus funciones y nivel de exposición al riesgo. Estas acciones estarán orientadas a fortalecer las competencias necesarias para su uso responsable, seguro y ético, así como el conocimiento de sus capacidades, limitaciones, riesgos, controles y responsabilidades.

11. VIGENCIA Y ACTUALIZACIÓN

La presente Política entra en vigor a partir de la fecha de su aprobación y publicación, y será revisada al menos cada dos años o cuando se produzcan cambios relevantes en la normativa, la estrategia corporativa, las tecnologías utilizadas o los riesgos asociados al uso de inteligencia artificial.