

	POLÍTICA	Código	Versión
		PO-IA-01	00
	Política de Inteligencia Artificial	Página	Vigencia
		1 de 11	05/05/2026

PLETTAC ELECTRONICS ARGENTINA S.A.
POLÍTICA DEL SISTEMA DE GESTIÓN DE INTELIGENCIA ARTIFICIAL
ISO/IEC 42001:2023

Código: PO-IA-01 | Versión: 00 | Vigencia: 05/05/2026 | Documento Base

Documento	Política del Sistema de Gestión de Inteligencia Artificial	Código	PO-IA-01
Sistema	Sistema de Gestión de Inteligencia Artificial - SGIA	Norma	ISO/IEC 42001:2023
Integración	Sistema de Gestión Integrado - SGI	Clasificación	Uso interno / Comunicación a partes interesadas pertinentes
Versión	00	Fecha de vigencia	05/05/2026
Elaboró	Responsable del SGI	Revisó	Dirección / IT / Seguridad de la Información / Desarrollo / Compliance
Aprobó	Dirección	Periodicidad de revisión	Anual o ante cambios significativos
Empresa	Plettac Electronics Argentina S.A.	Ámbito	República Argentina
Enfoque principal	Protección de información de clientes y uso seguro de IA	Aplicación	Uso interno, desarrollo e implementación de soluciones con IA

Este documento establece los compromisos, principios, lineamientos y responsabilidades para el uso, desarrollo, provisión, integración, implementación, operación y mejora de soluciones basadas en Inteligencia Artificial, con especial foco en la protección de la información de clientes y partes interesadas.

	POLÍTICA	Código	Versión
		PO-IA-01	00
	Política de Inteligencia Artificial	Página	Vigencia
		2 de 11	05/05/2026

Contenido del documento

1. Declaración de la política
2. Alcance de la política
3. Compromisos de la Dirección
4. Principios para el uso y gestión de la IA
5. Gobierno y protección de la información de clientes en IA
6. Uso de datos de clientes para desarrollo, pruebas, validación y mejora de IA
7. Controles para soluciones de IA que procesen información de clientes
8. Lineamientos de uso para colaboradores internos y externos
9. Uso de IA en procesos internos
10. Desarrollo, provisión e implementación de soluciones de IA
11. Gestión de proveedores y terceros con IA
12. Uso de IA en la relación con proveedores
13. Clasificación de usos de IA
14. Usos prohibidos de IA
15. Gestión de incidentes relacionados con IA
16. Competencia, capacitación y concientización
17. Comunicación a clientes y partes interesadas
18. Objetivos del SGIA
19. Seguimiento, auditoría y mejora continua
20. Cumplimiento obligatorio
21. Cierre institucional
22. Versión resumida de la política para comunicación externa
23. Historial de Cambios
24. Plan de Comunicación
25. Revisión y Aprobación

	POLÍTICA	Código	Versión
		PO-IA-01	00
	Política de Inteligencia Artificial	Página	Vigencia
		3 de 11	05/05/2026

1. Declaración de la política

Plettac Electronics Argentina S.A. reconoce a la Inteligencia Artificial (IA) como una tecnología estratégica para fortalecer la innovación, la calidad, la seguridad, la eficiencia operativa, la confiabilidad de sus soluciones y la mejora continua de sus procesos, productos y servicios.

En este marco, la organización establece, implementa, mantiene y mejora continuamente su Sistema de Gestión de Inteligencia Artificial (SGIA), conforme a los criterios de la norma ISO/IEC 42001:2023, con el propósito de asegurar que el uso, evaluación, selección, diseño, desarrollo, integración, implementación, validación, operación, monitoreo, mantenimiento y mejora de sistemas, herramientas, componentes, productos, servicios y soluciones que utilicen, incorporen o integren funcionalidades basadas en IA se realicen de manera responsable, segura, ética, transparente, controlada, trazable y confiable.

El SGIA aplica tanto al uso de herramientas de IA en los procesos internos de la organización como al desarrollo, provisión, integración, implementación, operación, mantenimiento y soporte de soluciones de IA destinadas a clientes públicos o privados. Las autorizaciones se documentarán según criticidad; los usos de nivel medio podrán ser aprobados por el responsable del proceso, los de nivel alto por Dirección o delegación formal tras evaluación técnica y del SGI, y los críticos por Dirección General tras evaluación multidisciplinaria de riesgos e impactos.

Las excepciones a requisitos que admitan excepción deberán justificarse, evaluarse por riesgo, documentarse, contar con controles compensatorios, plazo y aprobación de autoridad equivalente al nivel de riesgo. Ninguna excepción habilita incumplimientos legales, contractuales o usos prohibidos.

La Dirección de Plettac Electronics Argentina S.A. asume el compromiso de promover el uso responsable y seguro de la IA, proteger los datos e información de la organización, clientes y partes interesadas, gestionar los riesgos y oportunidades asociados a la IA, y asegurar que las actividades alcanzadas por el SGIA se desarrollen en cumplimiento de los requisitos legales, regulatorios, contractuales, normativos y del Sistema de Gestión Integrado (SGI).

2. Alcance de la política

La presente política aplica a todas las personas que realizan actividades para Plettac Electronics Argentina S.A. o en su nombre, incluyendo Dirección, empleados, colaboradores internos, colaboradores externos, contratistas, consultores, proveedores, integradores, socios tecnológicos y terceros que participen en procesos, productos, servicios o soluciones alcanzadas por el SGIA.

La política aplica, en particular, a:

- El uso de herramientas de IA en procesos internos.
- El diseño y desarrollo de software aplicado a sistemas de seguridad electrónica.
- El diseño, desarrollo, armado, configuración, integración o validación de hardware aplicado a sistemas de seguridad electrónica.
- La provisión, integración, implementación, operación, mantenimiento y soporte de sistemas de seguridad electrónica que utilicen o incorporen IA.
- El uso de IA generativa para documentación, análisis, desarrollo, soporte, pruebas, gestión de proyectos, gestión del SGI, asistencia técnica o mejora de procesos.
- La evaluación, adquisición, contratación, integración o uso de plataformas, modelos, APIs, servicios cloud, componentes, fabricantes o proveedores que incorporen IA.
- El tratamiento de datos, información, documentación técnica, contractual, comercial, operativa o de clientes mediante sistemas o herramientas de IA.
- El uso de IA en la gestión, evaluación, selección, homologación, seguimiento, comunicación y control de proveedores.

3. Compromisos de la Dirección

La Dirección de Plettac Electronics Argentina S.A. se compromete a:

- Establecer, implementar, mantener y mejorar continuamente el SGIA, asegurando su integración con el Sistema de Gestión Integrado de la organización.
- Alinear el SGIA con las normas ISO 9001, ISO 14001, ISO/IEC 27001, ISO 37001 e ISO 45001, y con los requisitos legales, regulatorios, contractuales y normativos aplicables.
- Promover un uso responsable, seguro, ético, transparente y confiable de la IA en los procesos internos, productos, servicios y soluciones de la organización.
- Proteger los datos e información de la organización, clientes, usuarios, proveedores y partes interesadas, evitando su exposición, uso indebido, pérdida, alteración, tratamiento no autorizado o divulgación.

	POLÍTICA	Código	Versión
		PO-IA-01	00
	Política de Inteligencia Artificial	Página	Vigencia
		4 de 11	05/05/2026

- Asegurar que la información de clientes sea tratada bajo criterios de minimización, necesidad, confidencialidad, autorización, trazabilidad, seguridad y control durante todo el ciclo de vida de la IA.
- Gestionar los riesgos y oportunidades asociados a la IA, considerando sus impactos sobre la seguridad de la información, privacidad, confidencialidad, calidad, continuidad operativa, cumplimiento legal, reputación, ética, derechos de las personas y confianza de los clientes.
- Asegurar que los sistemas, herramientas, productos, servicios y soluciones con IA sean evaluados, aprobados, validados, monitoreados y revisados conforme a su finalidad, criticidad, riesgos e impactos.
- Garantizar que los resultados generados o asistidos por IA cuenten con supervisión humana adecuada antes de ser utilizados en decisiones, entregables, productos, servicios, documentación contractual, documentación técnica, propuestas, registros del SGI o comunicaciones relevantes.
- Establecer reglas de uso de IA claras, comprensibles y obligatorias para colaboradores internos y externos.
- Asegurar la competencia, capacitación y concientización del personal y terceros pertinentes respecto del uso responsable, seguro y permitido de la IA.
- Evaluar y controlar a proveedores, fabricantes, plataformas, APIs, modelos, servicios cloud y terceros que desarrollen, suministren, integren, operen o mantengan soluciones con IA.
- Mantener registros y evidencias que permitan demostrar la trazabilidad, aprobación, validación, monitoreo, revisión, tratamiento de riesgos y mejora de los sistemas y usos de IA.
- Revisar periódicamente el desempeño del SGIA, sus objetivos, riesgos, controles, incidentes, no conformidades, resultados de auditoría y oportunidades de mejora.

4. Principios para el uso y gestión de la IA

4.1 Responsabilidad humana y organizacional

La IA es una herramienta de apoyo y no reemplaza la responsabilidad humana ni organizacional sobre los resultados, decisiones, productos, servicios, entregables o impactos generados. Toda salida, recomendación, análisis, código, diseño, configuración, documentación o decisión asistida por IA deberá ser revisada por personal competente cuando pueda impactar en clientes, usuarios, seguridad, privacidad, calidad, cumplimiento legal, continuidad operativa, reputación o desempeño del servicio.

4.2 Seguridad de la información

El uso de IA deberá preservar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información. Queda prohibido utilizar herramientas de IA para tratar información confidencial, restringida, sensible, contractual, técnica, comercial, personal o de clientes sin evaluación y autorización previa, y sin los controles de seguridad correspondientes.

4.3 Protección de datos y privacidad

El tratamiento de datos personales mediante IA deberá realizarse únicamente cuando exista una finalidad legítima, necesidad, proporcionalidad, autorización correspondiente y controles adecuados de seguridad, privacidad, minimización, confidencialidad, trazabilidad y cumplimiento legal. La organización deberá proteger especialmente los datos de clientes, usuarios finales, empleados, proveedores y terceros, evitando su uso indebido, exposición o procesamiento no autorizado en sistemas de IA.

4.4 Transparencia y trazabilidad

Los usos relevantes de IA deberán ser identificables, documentados y trazables. Cuando corresponda, se deberá conservar evidencia sobre finalidad, sistema o herramienta utilizada, datos o fuentes empleadas, responsable, evaluación de riesgos, validaciones realizadas, supervisión humana aplicada, resultados relevantes, decisiones adoptadas y controles implementados.

4.5 Calidad, confiabilidad y validación

Los sistemas, herramientas, productos, servicios y soluciones que incorporen IA deberán ser evaluados y validados respecto de su finalidad prevista, desempeño, precisión, limitaciones, robustez, seguridad, mantenibilidad, confiabilidad, riesgos e impactos antes de su uso productivo, integración o entrega a clientes.

4.6 Ética, integridad y uso legítimo

La IA deberá utilizarse de forma ética, íntegra y legítima. No deberá emplearse para manipular información, ocultar errores, alterar evidencias, generar documentación falsa, vulnerar controles, evadir responsabilidades, inducir a error a clientes o terceros, o realizar prácticas contrarias a la ley, la ética empresarial, la competencia leal o los compromisos antisoborno.

	POLÍTICA	Código	Versión
		PO-IA-01	00
	Política de Inteligencia Artificial	Página	Vigencia
		5 de 11	05/05/2026

4.7 No discriminación y prevención de sesgos

Cuando una solución de IA pueda afectar personas, usuarios, ciudadanos, trabajadores, clientes o terceros, se deberán evaluar y gestionar los riesgos de sesgo, discriminación, clasificación injustificada, exclusión, error sistemático o afectación negativa de derechos.

4.8 Supervisión humana

Los sistemas y herramientas de IA deberán contar con niveles adecuados de supervisión humana, especialmente cuando intervengan en decisiones, recomendaciones, análisis, diseños, configuraciones, alertas, productos o servicios que puedan tener impacto técnico, operativo, contractual, legal, económico, reputacional, de seguridad o sobre derechos de personas.

4.9 Gestión de riesgos y oportunidades

La organización deberá identificar, analizar, evaluar, tratar y monitorear los riesgos y oportunidades asociados al uso, desarrollo, provisión e integración de IA, considerando el ciclo de vida de los sistemas de IA, la seguridad de la información, la privacidad, la calidad, el cumplimiento legal, los requisitos contractuales y el impacto en las partes interesadas.

4.10 Mejora continua

El SGIA será revisado y mejorado periódicamente para asegurar su eficacia, adecuación, pertinencia y alineación con la estrategia organizacional, los avances tecnológicos, los requisitos legales, las expectativas de clientes, los resultados de auditoría, los incidentes, las no conformidades y el desempeño del SGI.

5. Gobierno y protección de la información de clientes en IA

La protección de la información de clientes constituye un requisito prioritario del SGIA. Plettac Electronics Argentina S.A. se compromete a preservar la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y uso autorizado de la información de clientes en todo uso, desarrollo, provisión, integración, operación, mantenimiento o soporte de soluciones basadas en IA.

La información de clientes comprende, entre otros activos, documentación técnica, planos, diseños, diagramas, configuraciones, información de infraestructura, datos de seguridad física o electrónica, contratos, propuestas, cotizaciones, pliegos, credenciales, registros operativos, incidentes, imágenes, video, audio, datos personales, información comercial, información económica, información de proyectos y cualquier otro dato entregado, generado, accedido o tratado por Plettac en el marco de una relación comercial, contractual, técnica u operativa. Para asegurar su protección, la organización establece que:

- La información de clientes no deberá ser utilizada en herramientas o sistemas de IA sin finalidad definida, necesidad justificada, autorización correspondiente y controles adecuados.
- No deberá cargarse información de clientes en herramientas públicas, personales, no aprobadas o no autorizadas de IA.
- Toda información de clientes deberá tratarse conforme a su clasificación, requisitos contractuales, acuerdos de confidencialidad, requisitos legales y controles de seguridad aplicables.
- Cuando sea posible, deberá utilizarse información anonimizada, seudonimizada, minimizada, segregada o sintética para reducir la exposición de datos reales de clientes.
- El acceso a información de clientes en entornos de IA deberá limitarse al personal autorizado, competente y con necesidad de acceso según su función.
- Los usos de IA que traten información de clientes deberán contar con trazabilidad suficiente para identificar finalidad, responsable, herramienta, datos utilizados, controles aplicados y resultados relevantes.
- La información de clientes no deberá utilizarse para entrenar, ajustar, mejorar o alimentar modelos de IA propios o de terceros sin autorización expresa, evaluación previa y controles documentados.
- Los proveedores, fabricantes, plataformas, servicios cloud, APIs o terceros que participen en el tratamiento de información de clientes mediante IA deberán ser evaluados y controlados conforme a los requisitos de seguridad, confidencialidad, privacidad, cumplimiento y trazabilidad definidos por la organización.
- Todo incidente, exposición, uso indebido, pérdida, alteración, divulgación o tratamiento no autorizado de información de clientes relacionado con IA deberá ser reportado y gestionado conforme a los procedimientos internos aplicables.

6. Uso de datos de clientes para desarrollo, pruebas, validación y mejora de IA

El uso de datos de clientes en actividades de desarrollo, pruebas, validación, entrenamiento, ajuste, monitoreo, soporte, mantenimiento o mejora de sistemas de IA deberá ser excepcional, justificado, autorizado y controlado. La regla general será evitar el uso de datos reales de clientes cuando puedan emplearse datos sintéticos, anonimizados, seudonimizados o conjuntos de prueba controlados.

	POLÍTICA	Código	Versión
		PO-IA-01	00
	Política de Inteligencia Artificial	Página	Vigencia
		6 de 11	05/05/2026

Antes de utilizar datos de clientes en cualquier actividad relacionada con IA, se deberá verificar y documentar, según corresponda:

- La finalidad específica del uso de datos.
- La base contractual, legal o autorización aplicable.
- El tipo de datos involucrados y su nivel de clasificación.
- La existencia de datos personales, datos sensibles o información crítica de seguridad.
- La necesidad y proporcionalidad del tratamiento.
- La posibilidad de aplicar minimización, anonimización, seudonimización, tokenización, enmascaramiento o uso de datos sintéticos.
- La herramienta, plataforma, modelo, proveedor o entorno tecnológico donde serán tratados los datos.
- La ubicación del procesamiento, almacenamiento y posibles transferencias.
- Los controles de acceso, registro, cifrado, retención, eliminación y segregación aplicables.
- Los riesgos de exposición, uso indebido, reidentificación, fuga, sesgo, error o reutilización no autorizada.
- La revisión y aprobación del responsable del proceso, Seguridad de la Información, Compliance, Legales o Dirección, según la criticidad.

Los datos de clientes utilizados en actividades de IA deberán conservarse solo durante el tiempo necesario para la finalidad autorizada y deberán ser eliminados, anonimizados o protegidos conforme a los criterios definidos por la organización, los contratos aplicables y la legislación vigente.

7. Controles para soluciones de IA que procesen información de clientes

Toda solución de IA desarrollada, integrada, provista, implementada, mantenida u operada por Plettac que procese información de clientes deberá incorporar controles proporcionales a su criticidad, finalidad, contexto de uso, tipo de datos, impacto potencial y requisitos contractuales.

Como mínimo, deberán evaluarse y aplicarse, cuando corresponda, los siguientes controles:

- Definición documentada de la finalidad de la solución de IA y límites de uso permitidos.
- Identificación de los datos de clientes requeridos, fuentes utilizadas, flujos de información y responsables del tratamiento.
- Evaluación de riesgos e impactos antes de la implementación, puesta en producción o entrega al cliente.
- Validación funcional, técnica, de seguridad, privacidad, calidad y desempeño antes de liberar la solución.
- Supervisión humana adecuada sobre resultados, alertas, recomendaciones, clasificaciones, análisis o decisiones asistidas por IA.
- Controles de acceso, autenticación, autorización, segregación de ambientes, registro de actividad y trazabilidad de operaciones.
- Protección contra exposición no autorizada, extracción indebida, fuga de información, uso no autorizado para entrenamiento o transferencia a terceros.
- Gestión de cambios, actualizaciones, ajustes, reentrenamientos, nuevas versiones, integraciones o modificaciones relevantes.
- Definición de criterios de aceptación, limitaciones conocidas, supuestos, condiciones de uso, responsabilidades y requisitos de mantenimiento.
- Mecanismos para reportar, analizar y tratar incidentes, errores, sesgos, resultados inesperados, pérdida de desempeño o desviaciones relevantes.
- Evaluación de proveedores, fabricantes, componentes, modelos, APIs o servicios cloud que intervengan en la solución.
- Conservación de registros y evidencias que demuestren evaluación, aprobación, validación, monitoreo, revisión y mejora.

Cuando corresponda por contrato, criticidad o naturaleza del servicio, Plettac informará al cliente sobre el uso de componentes o funcionalidades de IA, sus responsabilidades, limitaciones relevantes, controles aplicados y requisitos de uso seguro.

8. Lineamientos de uso para colaboradores internos y externos

Toda persona que utilice IA en nombre de Plettac Electronics Argentina S.A. deberá cumplir los siguientes lineamientos:

	POLÍTICA	Código	Versión
		PO-IA-01	00
	Política de Inteligencia Artificial	Página	Vigencia
		7 de 11	05/05/2026

- Utilizar únicamente herramientas, plataformas, modelos, APIs o servicios de IA aprobados o autorizados por la organización para la finalidad correspondiente.
- No cargar en herramientas de IA información confidencial, restringida, sensible, contractual, técnica, comercial, personal, financiera, de seguridad, de clientes o de proveedores, salvo autorización formal y controles adecuados.
- No cargar credenciales, contraseñas, claves, tokens, certificados, secretos, configuraciones sensibles, código fuente propietario no autorizado, vulnerabilidades no divulgadas o información que pueda comprometer la seguridad de la organización o de clientes.
- No utilizar datos reales de clientes para pruebas, entrenamiento, validación, soporte o mejora de IA sin autorización y controles documentados.
- Revisar críticamente los resultados generados por IA antes de utilizarlos, compartirlos, incorporarlos a entregables o tomar decisiones basadas en ellos.
- No presentar contenidos generados por IA como definitivos, validados, aprobados o auditados sin revisión humana competente.
- No utilizar IA para generar información falsa, engañosa, discriminatoria, ofensiva, fraudulenta, ilegal o contraria a las políticas internas.
- No utilizar IA para manipular, alterar u ocultar registros, evidencias de auditoría, reportes técnicos, resultados de pruebas, documentación contractual, documentación comercial o registros del SGI.
- Reportar al Responsable del SGI, Seguridad de la Información, IT o responsable designado cualquier incidente, sospecha de exposición de datos, resultado incorrecto relevante, uso indebido, comportamiento inesperado, vulnerabilidad o incumplimiento relacionado con IA.
- Participar en las capacitaciones y actividades de concientización definidas por la organización.
- Cumplir con los procedimientos, instructivos, autorizaciones y controles establecidos para el uso responsable y seguro de IA.

9. Uso de IA en procesos internos

La organización podrá utilizar herramientas de IA en sus procesos internos para mejorar la eficiencia, calidad, análisis, documentación, soporte, automatización y gestión del conocimiento, siempre que se respeten los requisitos de esta política y los controles aplicables.

Los usos internos de IA deberán tener una finalidad definida, estar autorizados según su criticidad, ser evaluados cuando traten información confidencial, sensible, personal o de clientes, contar con revisión humana cuando sus resultados impacten en decisiones o entregables relevantes, mantener evidencias cuando impacten en procesos críticos y respetar las políticas de seguridad de la información, confidencialidad, protección de datos, uso aceptable de recursos tecnológicos, ética y compliance.

10. Desarrollo, provisión e implementación de soluciones de IA

Cuando Plettac Electronics Argentina S.A. diseñe, desarrolle, integre, implemente, provea, mantenga o soporte soluciones que incorporen IA, deberá asegurar que:

- La finalidad del sistema o funcionalidad de IA esté definida y documentada.
- Se identifiquen los usuarios, clientes, partes interesadas y posibles afectados por la solución.
- Se evalúen los riesgos e impactos asociados al uso previsto y al uso indebido razonablemente previsible.
- Se definan controles de seguridad, privacidad, calidad, trazabilidad, supervisión humana y gestión de errores.
- Se validen el desempeño, confiabilidad, limitaciones y criterios de aceptación antes de la puesta en producción o entrega al cliente.
- Se documenten los supuestos, restricciones, condiciones de uso, dependencias, datos requeridos, proveedores involucrados y responsabilidades.
- Se asegure que el sistema de IA sea mantenible, monitoreable y revisable durante su ciclo de vida.
- Se gestionen los cambios, actualizaciones, reentrenamientos, ajustes, nuevas versiones o modificaciones relevantes.
- Se definan mecanismos para reportar, analizar y tratar incidentes, errores, resultados inesperados, sesgos o desviaciones de desempeño.
- Se establezcan acuerdos contractuales, técnicos y operativos claros cuando participen clientes, proveedores, fabricantes, integradores o terceros.

11. Gestión de proveedores y terceros con IA

	POLÍTICA	Código	Versión
		PO-IA-01	00
	Política de Inteligencia Artificial	Página	Vigencia
		8 de 11	05/05/2026

Todo proveedor, fabricante, integrador, consultor, plataforma, servicio cloud, API, modelo, herramienta o tercero que provea, desarrolle, integre, procese, opere o mantenga funcionalidades de IA deberá ser evaluado según su criticidad y riesgo.

La evaluación deberá considerar, cuando corresponda:

- Finalidad del servicio o componente de IA.
- Tipo de IA utilizada.
- Datos tratados, especialmente si incluyen información de clientes o datos personales.
- Ubicación del procesamiento y almacenamiento.
- Condiciones de confidencialidad.
- Uso o no de datos para entrenamiento, mejora o ajuste de modelos.
- Controles de seguridad de la información.
- Controles de privacidad y protección de datos.
- Trazabilidad y registros disponibles.
- Desempeño, disponibilidad y continuidad del servicio.
- Propiedad intelectual y licenciamiento.
- Soporte ante incidentes.
- Subcontratistas involucrados.
- Requisitos contractuales y regulatorios.
- Certificaciones, auditorías, informes o evidencias de control disponibles.

No deberán utilizarse proveedores o herramientas de IA para información crítica, confidencial, sensible o de clientes sin evaluación y autorización previa.

12. Uso de IA en la relación con proveedores

Plettac Electronics Argentina S.A. podrá utilizar herramientas de IA como apoyo en los procesos de gestión, evaluación, selección, homologación, seguimiento, comunicación, análisis documental, análisis de riesgos, comparación de ofertas y control de proveedores, siempre que dicho uso se realice de manera responsable, segura, trazable y conforme a los requisitos definidos por el SGIA, el SGI y la legislación aplicable.

La IA no deberá ser utilizada como único criterio de decisión para la selección, aprobación, rechazo, sanción o desvinculación de proveedores. Toda decisión relevante deberá contar con revisión, validación y aprobación humana por parte del personal competente.

No se deberá cargar en herramientas de IA información confidencial, sensible, contractual, técnica, comercial, económica, financiera, personal o estratégica de proveedores sin autorización, finalidad definida y controles adecuados. Cuando un proveedor utilice IA para prestar servicios, desarrollar componentes, procesar información o integrar soluciones para Plettac o sus clientes, deberá declararlo y someterse a la evaluación correspondiente conforme a los requisitos del SGIA.

El uso de IA en la relación con proveedores deberá prevenir sesgos, errores, conflictos de interés, manipulación de información, afectación a la competencia leal, incumplimientos contractuales o prácticas contrarias a la ética y al Sistema de Gestión Antisoborno.

13. Clasificación de usos de IA

La organización deberá clasificar los usos, herramientas, sistemas o soluciones de IA según su criticidad y riesgo, documentándolos en RG-IA-01 — Inventario de Sistemas y Casos de Uso de Inteligencia Artificial. El registro identificará las herramientas y los casos de uso, su situación de autorización y restricciones aplicables, sin reproducir su información en esta política. La identificación en RG-IA-01 no constituye autorización automática. Se consideran como mínimo las categorías siguientes:

Nivel	Descripción	Requisito mínimo
Bajo	Uso auxiliar sin información confidencial ni impacto relevante.	Autorizado en RG-IA-01; revisión.
Medio	Uso con información interna o apoyo a procesos relevantes.	Aprueba líder del proceso.
Alto	Uso con información confidencial, clientes, datos personales, productos o servicios.	Eval. técnica y SGI; Dirección/delegado.
Crítico	Uso con impacto en seguridad, derechos de personas, infraestructura crítica, decisiones relevantes o clientes públicos.	Eval. de impacto; Dirección General.

	POLÍTICA	Código	Versión
		PO-IA-01	00
	Política de Inteligencia Artificial	Página	Vigencia
		9 de 11	05/05/2026

14. Usos prohibidos de IA

Queda prohibido:

- Cargar credenciales, contraseñas, claves, tokens, certificados, secretos o configuraciones sensibles en herramientas de IA.
- Cargar información confidencial, restringida, contractual, técnica, comercial, personal o de clientes en herramientas públicas, no aprobadas o sin autorización.
- Utilizar información de clientes para entrenar, ajustar, probar o mejorar modelos de IA sin autorización, base legal, controles y acuerdos correspondientes.
- Utilizar IA para vulnerar sistemas, evadir controles de seguridad, generar código malicioso, explotar vulnerabilidades o facilitar actividades no autorizadas.
- Utilizar IA para suplantar identidades, generar comunicaciones engañosas, simular aprobaciones, falsificar evidencias o inducir a error a clientes, autoridades, proveedores o personal interno.
- Utilizar IA para alterar, ocultar, fabricar o manipular registros del SGI, evidencias de auditoría, resultados de pruebas, reportes técnicos, documentos contractuales o información de cumplimiento.
- Presentar contenido generado por IA como definitivo, validado, aprobado o emitido oficialmente sin revisión humana competente.
- Incorporar funcionalidades de IA en productos, servicios o soluciones para clientes sin evaluación de riesgos, validación y aprobación correspondiente.
- Utilizar IA para realizar prácticas discriminatorias, ilegales, fraudulentas, antisoborno, anticompetitivas o contrarias a la ética empresarial.
- Utilizar herramientas de IA que incumplan requisitos mínimos de seguridad, confidencialidad, privacidad, trazabilidad o cumplimiento definidos por la organización.

15. Gestión de incidentes relacionados con IA

Todo incidente, sospecha, uso indebido, comportamiento inesperado, falla, sesgo, resultado incorrecto relevante, exposición de información, incumplimiento, vulnerabilidad o afectación relacionada con IA deberá ser reportado y tratado conforme a los procedimientos internos aplicables.

Los incidentes relacionados con IA podrán incluir, entre otros:

- Carga indebida de información confidencial o de clientes.
- Uso de herramientas de IA no autorizadas.
- Pérdida de trazabilidad.
- Resultado incorrecto utilizado en un entregable.
- Falla de una funcionalidad de IA en una solución provista.
- Comportamiento discriminatorio o sesgado.
- Exposición de datos personales.
- Vulnerabilidad de seguridad.
- Uso indebido de código, documentación o propiedad intelectual.
- Incumplimiento contractual o legal.
- Uso no ético o contrario a esta política.

16. Competencia, capacitación y concientización

Plettac Electronics Argentina S.A. deberá asegurar que las personas que participan en actividades relacionadas con IA posean la competencia necesaria según sus funciones, responsabilidades y nivel de exposición al riesgo. La organización desarrollará actividades de capacitación y concientización orientadas a comprender los beneficios, riesgos y limitaciones de la IA; conocer usos permitidos, restringidos y prohibidos; proteger información confidencial y datos de clientes; evitar la exposición de datos en herramientas no autorizadas; aplicar revisión humana; identificar sesgos, errores o resultados no confiables; reportar incidentes; y cumplir los procedimientos y controles del SGIA.

La capacitación será aplicable a colaboradores internos y, cuando corresponda, a colaboradores externos, proveedores, contratistas o terceros que participen en actividades alcanzadas por el SGIA.

17. Comunicación a clientes y partes interesadas

	POLÍTICA	Código	Versión
		PO-IA-01	00
	Política de Inteligencia Artificial	Página	Vigencia
		10 de 11	05/05/2026

Plettac Electronics Argentina S.A. publicará la versión vigente de esta Política de Inteligencia Artificial para conocimiento general de los colaboradores, socios comerciales y demás partes interesadas pertinentes, por los canales institucionales definidos. Su finalidad es difundir los compromisos y principios del SGIA; no se requiere firma individual de esta política. El Responsable del SGI coordinará publicación, disponibilidad, actualización y evidencia de comunicación.

La organización podrá informar a sus clientes que cuenta con un Sistema de Gestión de Inteligencia Artificial alineado a ISO/IEC 42001:2023, gestiona riesgos e impactos asociados al uso y desarrollo de IA, protege la información y los datos de clientes, no utiliza datos de clientes en herramientas de IA sin autorización y controles adecuados, evalúa proveedores y componentes de IA, aplica supervisión humana, validación, trazabilidad y mejora continua sobre soluciones con IA, y gestiona incidentes y no conformidades relacionados con IA.

18. Objetivos del SGIA

La organización establecerá objetivos medibles del SGIA, coherentes con esta política, el alcance definido, los riesgos y oportunidades identificados, y los objetivos del SGI.

Los objetivos podrán estar relacionados con identificación e inventario de usos y sistemas de IA, evaluación de riesgos e impactos, protección de datos e información de clientes, capacitación y concientización, evaluación de proveedores, validación y monitoreo de soluciones con IA, reducción de incidentes, mejora de trazabilidad y supervisión humana, y cumplimiento legal, contractual y normativo.

19. Seguimiento, auditoría y mejora continua

El cumplimiento de esta política será verificado mediante seguimiento de objetivos e indicadores del SGIA, auditorías internas, evaluaciones de riesgos e impactos, revisión de incidentes, no conformidades y acciones correctivas, evaluación de proveedores y terceros, revisión de cambios tecnológicos, legales o contractuales, revisión por la Dirección y mejora continua del SGIA.

La política será revisada periódicamente o cuando se produzcan cambios relevantes en el contexto organizacional, alcance del SGIA, tecnologías utilizadas, requisitos legales, requisitos de clientes, riesgos identificados, incidentes, resultados de auditoría o desempeño del sistema.

20. Cumplimiento obligatorio

El cumplimiento de esta política es obligatorio para todas las personas alcanzadas por el SGIA. El incumplimiento podrá dar lugar a acciones correctivas, restricciones de acceso, suspensión de uso de herramientas de IA, revisión de responsabilidades, medidas disciplinarias, medidas contractuales o las acciones que correspondan según la normativa interna, la legislación aplicable y los acuerdos vigentes.

21. Cierre institucional

Plettac Electronics Argentina S.A. se compromete a desarrollar, integrar, proveer y utilizar soluciones basadas en Inteligencia Artificial de manera responsable, segura, ética y confiable, asegurando que la IA contribuya a la innovación, la calidad, la protección de la información, la confianza de los clientes, el cumplimiento legal, la integridad empresarial y la mejora continua del Sistema de Gestión Integrado.

22. Versión resumida de la política para comunicación externa.

Plettac Electronics Argentina S.A. gestiona el uso, desarrollo e implementación de soluciones basadas en Inteligencia Artificial mediante un Sistema de Gestión de Inteligencia Artificial alineado a ISO/IEC 42001:2023.

23. Historial de Cambios

Versión	Tipo de Cambio	Autor	Solicitante Usuario /Referente	Fecha de Modificación	Descripción Breve
V.00	Doc. Base	Res. Del SGI	Dirección	05/05/2026	Documento Base Nuevo

	POLÍTICA	Código	Versión
		PO-IA-01	00
	Política de Inteligencia Artificial	Página	Vigencia
		11 de 11	05/05/2026

24. Plan de Comunicación

Qué comunicar	Cuando comunicar	A quién comunicar	Cómo comunicar	Quién comunica
Política vigente	Desde vigencia	Colaboradores y socios comerciales	Publicación institucional	Responsable del SGI
Cambios	Tras aprobación	Destinatarios pertinentes	Publicación actualizada	Responsable del SGI

25. Revisión y Aprobación

Elaboró	Revisó	Aprobó
Responsable del SGI (Juan Sanchez)	Oficial de Cumplimiento (Federico Toma)	Dirección (Guido Bronssilovsky)