



INTELIGO PERÚ HOLDINGS

Política de Gobernanza de datos con IA

PROCESOS Y CALIDAD

Política de Gobernanza de datos con IA

Indice

1. Objetivo	1
2. Alcance	1
3. Referencias	1
4. Responsables	1
5. Definiciones	4
6. Principios	4
7. Administración de la política	5
8. Lineamientos para la Política de Gobernanza de datos con IA	6
9. Sanciones	8
Anexos	9
Control de cambios	10

Este documento contiene información de propiedad de Inteligo IPH. Antes de utilizarlo, verifique que la versión esté vigente a fin de evitar su uso indebido. De ser éste un documento de uso confidencial, no podrá ser objeto de reproducción total o parcial, tratamiento informático ni transmisión de ninguna forma sin autorización previa de Inteligo IPH.

Versión 1.0

Fecha de aprobación: 13/01/2026 | Revisado por: Procesos y Calidad

Fecha de vigencia: 21/07/2025

1. Objetivo

Establecer los lineamientos generales para la gobernanza de datos con Inteligencia Artificial (IA), con el fin de prevenir y controlar el impacto de estos.

2. Alcance

La gobernanza de datos con IA está dirigida a todo el personal que utilice la Inteligencia Artificial en sus actividades diarias.

3. Referencias

- Ley N° 31814 — Ley que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país
- Ley N° 29733 — Ley de Protección de Datos Personales
- Reglamento de la Ley N° 31814, Ley que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país
- Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales
- NIST AI 100-1 - Artificial Intelligence Risk Management Framework (AI RMF 1.0)
- NTP-ISO/IEC 27002:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información
- NTP-ISO/IEC 42001:2025 - Tecnología de la información. Inteligencia artificial. Sistema de gestión
- IPH-SGSI-PO-001 Política de Seguridad de la Información y Ciberseguridad

4. Responsables

El Oficial de Seguridad de la Información es responsable de:

- Divulgar la presente política con los colaboradores de la empresa.
- Supervisar y aprobar la documentación relacionada con la presente política.

El analista de Seguridad de la Información es responsable de:

- Revisión de las páginas de IA seguras y permitidas por parte de la empresa.
- Actualización de la presente política según las necesidades de la empresa
- Apoyar a los colaboradores en caso de dudas en el tipo de información a utilizar.

Los colaboradores son responsables de:

- Hacer uso correcto de la información a utilizar dentro de las páginas de IA.
- No utilizar información confidencial dentro de dichas páginas y/o repositorios.
- Utilizar información clasificada como pública, evitando el uso de los datos personales de los colaboradores y/o clientes.

Este documento contiene información de propiedad de Inteligo IPH. Antes de utilizarlo, verifique que la versión esté vigente a fin de evitar su uso indebido. De ser éste un documento de uso confidencial, no podrá ser objeto de reproducción total o parcial, tratamiento informático ni transmisión de ninguna forma sin autorización previa de Inteligo IPH.

Versión 1.0

Fecha de aprobación: 13/01/2026 | Revisado por: Procesos y Calidad

Fecha de vigencia: 21/07/2025

5. Definiciones

Inteligencia Artificial (IA): se define como la tecnología que permite a sistemas informáticos realizar tareas que normalmente requieren inteligencia humana, como el análisis de datos, la toma de decisiones, el reconocimiento de patrones y la automatización de procesos.

Datos Personales: se define como cualquier información que identifica o puede identificar a una persona natural, esto incluye datos como el nombre, número de documento de identidad, dirección, correo electrónico, número de teléfono, entre otros.

Datos Sensibles: se define como información que se refiere a aspectos íntimos de una persona y cuya divulgación o uso indebido podría afectar su privacidad o generar discriminación. Esto incluye información como el origen racial o étnico, opiniones políticas, convicciones religiosas o filosóficas, estado de salud, orientación sexual, entre otros.

Ciclo de Vida de los datos: se define como las etapas por el que los datos se trasladan entre diferentes etapas desde que se generan o recolectan hasta que se eliminan o archivan los datos.

Minimización de Datos: se define como el principio que establece que se debe de recolectar, utilizar y/o procesar los datos estrictamente necesarios para el fin específico.

6. Principios

No discriminación: Se implementan medidas en las fases de desarrollo, implementación y uso de los sistemas basados en IA para prevenir, mitigar y corregir la generación, reforzamiento o perpetuación de resultados discriminatorios o sesgados. Los sistemas basados en IA deben ser utilizados de manera segura, responsable, ética, justa, transparente, equitativa y respetuosa de los derechos humanos.

Privacidad de datos personales: La protección de la privacidad y los datos personales en el desarrollo, implementación y uso de la IA requiere la implementación de medidas técnicas, organizativas y legales para preservar la seguridad de los datos, promover la transparencia de su tratamiento y fortalecer la confianza digital.

Protección de derechos fundamentales: La implementación y uso de los sistemas basados en IA deben garantizar el respeto y protección de los derechos fundamentales, así como el bienestar humano.

Respeto del derecho de autor y derechos conexos: Las fases del desarrollo, implementación y uso de los sistemas basados en IA deben respetar los derechos de autor, tanto morales como patrimoniales, así como de los creados respecto de sus obras originales.

Seguridad, proporcionalidad y fiabilidad: La fiabilidad y seguridad de los sistemas basados en IA debe estar presente en todas las fases de su desarrollo, implementación y uso, a fin de que funcionen adecuadamente y se mitiguen los riesgos del uso indebido. Las medidas adoptadas de las salvaguardias y medidas de fiabilidad y seguridad deben ser proporcionales al nivel de riesgo que el sistema basado en IA puede generar.

Sensibilización y educación en IA: Se promueve la alfabetización digital y desarrollo de habilidades relacionadas con el diseño, desarrollo, implementación y uso de sistemas basados en IA, así como la sensibilización y comprensión sobre su uso e impacto da riesgo.

Sostenibilidad: Las repercusiones humanas, sociales, económicas, culturales y ambientales deben analizarse y evaluarse en las fases del desarrollo, implementación y uso de los sistemas basados en IA, verificando su alineación con los objetivos de las políticas nacionales y objetivos de desarrollo sostenible (ODS) de las Naciones Unidas. Asimismo, se promueve la adopción de prácticas sostenibles que minimicen el consumo de energía y recursos, y fomenten soluciones tecnológicas responsables con el ambiente y comprometidas con el desarrollo sostenible.

Supervisión humana: Es necesario que los sistemas basados en IA estén supervisados por las personas responsables de su desarrollo, a fin de asegurar decisiones éticas, justas y respetuosas de los derechos fundamentales, así como de la calidad de los datos, asegurando su fiabilidad, precisión, integridad y representatividad. Los responsables del desarrollo de los sistemas basados en IA deben monitorear su desempeño para evaluar el impacto que ocasionan en los grupos de interés y corregir errores o consecuencias no deseadas de manera oportuna, en cumplimiento de los principios jurídicos, éticos y morales.

Transparencia: La transparencia fortalece la equidad, justicia y respeto a los derechos humanos. Los sistemas basados en IA deben ser claros, explicables y accesibles, garantizando procesos, algoritmos y decisiones comprensibles para usuarios, implementadores y autoridades. Esto incluye información sobre su funcionamiento, datos utilizados, criterios de decisión y posibles sesgos, promoviendo rendición de cuentas y confianza pública.

Rendición de cuentas: Los sistemas basados en IA son herramientas complementarias que ayudan a tomar decisiones, pero no reemplazan la experiencia y juicio de los responsables de su desarrollo, implementación y uso, quienes siguen siendo responsables respecto a eventuales usos impropios, ético e ilegales. Para ello deben garantizar mediante mecanismos que permitan identificar, evaluar y responder por los impactos generados por la IA, positivos y negativos, respecto de derechos humanos, equidad, confianza, seguridad y medio ambiente.

Desarrollo ético para una IA responsable: En el desarrollo, implementación y uso de los sistemas basados en IA se promueve el respeto de los derechos humanos, la dignidad, bienestar colectivo, conforme a los valores y principios éticos de nuestra organización.

Estándares de seguridad basados en riesgos: Se debe evaluar los riesgos específicos e implicancias en el desarrollo, implementación y uso de los sistemas basados en IA, identificando amenazas, vulnerabilidades y posibles consecuencias negativas, probabilidad de ocurrencia y el impacto asociado a cada riesgo.

7. Administración de la política

Es responsabilidad del Oficial de Seguridad de la Información revisar y de ser necesario modificar esta política una vez al año.

8. Lineamientos para la Política de Gobernanza de datos con IA

8.1. Generalidades

- Cada colaborador es responsable del manejo de la información dentro de las herramientas de IA, asegurándose de que no contenga datos confidenciales ni comprometa la privacidad de colaboradores, clientes, proveedores y/o cualquier titular del dato personal de quien la empresa tenga información.
- Es fundamental verificar cuidadosamente la información compartida en las herramientas de IA, asegurando que esté libre de sesgos que puedan distorsionar los resultados esperados.
- El acceso a las herramientas de IA debe restringirse exclusivamente a aquellas autorizadas por la empresa, con el objetivo de minimizar la exposición de datos corporativos y garantizar la seguridad de la información.
- En caso de emplear una herramienta de IA no autorizada por la empresa, esta deberá pasar por evaluación del equipo de Data Office y Seguridad de la Información, a fin de verificar el tipo de uso y la existencia de controles adecuados para la protección de la información, requisito indispensable para su aprobación.
- El uso de las herramientas de IA debe estar alineado con las políticas de seguridad de la información, gestión de riesgos y normativas legales, garantizando el cumplimiento de los estándares establecidos y evitando posibles sanciones por parte de los entes reguladores.
- Toda información generada mediante IA debe ser verificada y contrastada con fuentes confiables, ya que puede contener errores y no debe considerarse automáticamente como precisa o definitiva.
- La información compartida con sistemas de inteligencia artificial deberá limitarse exclusivamente a aquella etiquetada como de dominio público o de uso interno.
- Queda expresamente prohibida la divulgación y/o el tratamiento de datos personales o sensibles mediante sistemas de inteligencia artificial, salvo en casos excepcionales en los que exista consentimiento previo, expreso e inequívoco por parte del titular de dichos datos, debiendo además especificarse de manera clara la finalidad para la cual serán utilizados.
- Los sistemas basados en IA deberán tener una evaluación de riesgos previo a su uso y/o lanzamiento. Los colaboradores estarán sujetos a la revisión de los datos compartidos con la IA, con el propósito de verificar el uso adecuado de la información corporativa. En caso de detectarse un uso indebido, podrán ser sancionados conforme a las normativas establecidas por la empresa.
- Cuando la información generada mediante IA sea utilizada con fines divulgativos, se deberá indicar expresamente que fue creada por inteligencia artificial, garantizando transparencia en su origen y uso.
- Se deben implementar controles de seguridad, privacidad y transparencia, entre otros, para realizar una evaluación basada en riesgos sobre los sistemas que utilizan inteligencia artificial, garantizando la protección de los datos, la transparencia ética, la seguridad y la fiabilidad en su desarrollo, implementación y uso. Asimismo, se deberán establecer auditorías periódicas sobre los datos compartidos con dichas herramientas, asegurando el cumplimiento de los estándares de seguridad y privacidad.

Este documento contiene información de propiedad de Inteligo IPH. Antes de utilizarlo, verifique que la versión esté vigente a fin de evitar su uso indebido. De ser éste un documento de uso confidencial, no podrá ser objeto de reproducción total o parcial, tratamiento informático ni transmisión de ninguna forma sin autorización previa de Inteligo IPH.

Versión 1.0

Fecha de aprobación: 13/01/2026 | Revisado por: Procesos y Calidad

Fecha de vigencia: 21/07/2025

8.2. Uso de Inteligencia Artificial de Riesgo Alto

Se considera como uso de alto riesgo de los sistemas de inteligencia artificial aquel que suponga un riesgo para la vida humana, la dignidad, la libertad, la seguridad física u otros derechos fundamentales, ya sea por los objetivos perseguidos o por las consecuencias no deseadas de su implementación. No obstante, dicho uso podrá ser autorizado siempre que se cumplan estrictamente las condiciones y controles establecidos para mitigar dichos riesgos.

Dentro de los supuestos previstos por la regulación, se clasifica como uso de inteligencia artificial de riesgo alto en los siguientes escenarios:

- Determinar los procesos relacionados con la gestión del talento humano, incluyendo la selección, evaluación, contratación y cese de colaboradores o postulantes, así como la definición y aplicación de condiciones laborales.
- Determinar el perfil de riesgo o de inversión de los clientes con el uso de IA, salvo cuando su finalidad sea exclusivamente para la detección de fraude financiero.
- Cualquier aplicación que represente un riesgo para la vida humana, la integridad física, los derechos fundamentales, la libertad o la dignidad; así como aquellas cuyo uso conlleve una alta probabilidad de generar discriminación, estigmatización, sesgos culturales, o que implique alta complejidad para la supervisión humana.

Los sistemas basados en inteligencia artificial clasificados como de riesgo alto pasarán por un análisis de impacto previo, con el objetivo de identificar, evaluar y minimizar los riesgos potenciales asociados a su implementación. En caso de que dichos riesgos no puedan ser eliminados, se establecerán planes de acción específicos orientados a mitigar su posible materialización. Dichos procedimientos deberán ser documentados y actualizados por un periodo mínimo de tres (3) años, con el fin de contar con evidencia verificable en caso de requerimiento por parte de entidades gubernamentales o autoridades competentes.

8.3. Uso Indebido

Se considerará un uso indebido de los sistemas de IA aquel que genere un impacto irreversible, significativo y negativo sobre los derechos fundamentales o el bienestar de las personas, motivo por el cual su utilización se encuentra prohibida.

Se entenderá como uso indebido de la IA en los casos siguientes:

- Manipular o influir deliberadamente de manera engañosa o manipulativa en procesos de toma de decisiones, con el propósito de alterar la capacidad de decisión y juicio de una persona o grupo de personas; aprovechar vulnerabilidades cognitivas, emocionales o socioeconómicas para influir sustancialmente en su comportamiento; e inducir a error o manipular información utilizando sistemas basados en IA para afectar la autonomía de decisión
- Desarrollar o implementar capacidad letal autónoma, que comprenda toma de decisiones sin supervisión humana, que puedan ocasionar daño físico o afectar la vida o la integridad de las personas.
- Implementar sistemas de vigilancia masiva sin base legal o cuando estos puedan generar un impacto desproporcionado en el ejercicio de los derechos fundamentales.

Este documento contiene información de propiedad de Inteligo IPH. Antes de utilizarlo, verifique que la versión esté vigente a fin de evitar su uso indebido. De ser éste un documento de uso confidencial, no podrá ser objeto de reproducción total o parcial, tratamiento informático ni transmisión de ninguna forma sin autorización previa de Inteligo IPH.

Versión 1.0

Fecha de aprobación: 13/01/2026 | Revisado por: Procesos y Calidad

Fecha de vigencia: 21/07/2025

- Procesar, clasificar o inferir datos sensibles de individuos mediante datos biométricos para determinar o inferir su origen racial o étnico, ideología política, afiliación sindical, creencias religiosas o filosóficas, vida sexual u orientación sexual. Igualmente, realizar evaluaciones o clasificaciones de personas o grupos, sin importar el tipo de dato utilizado, cuando estas generen resultados discriminatorios o desproporcionados que afecten derechos fundamentales.
- Predecir que una persona cometa un delito sobre la base de un perfil físico de la persona o en sus rasgos y características de su personalidad.
- Emplear IA para actividades ilícitas, malintencionadas o incompatibles con el Código de Ética, el Código de Ética y Conducta de Proveedores, las Normas Internas de Conducta y demás normativas aplicables, tales como vigilancia indebida, manipulación de información, fraude, ciberdelitos o vulneración de derechos de propiedad intelectual.
- La empresa deberá realizar una evaluación previa a fin de evitar que los sistemas basados en IA sean utilizados para los supuestos indicados en la presente sección.

Se puede categorizar utilizando identificación biométrica en los siguientes casos:

- Realizar verificación biométrica solo para autenticación digital.
- Llevar a cabo investigaciones preliminares en casos de delitos graves que afecten la vida, el cuerpo, la salud, la libertad, el patrimonio, la administración pública, así como en delitos vinculados al lavado de activos, tráfico ilícito de drogas y minería ilegal.

9. Sanciones

El incumplimiento de la presente política resultará en sanciones y medidas disciplinarias a colaboradores de acuerdo con el Código de Ética y Conducta o las regulaciones aplicables.

Anexos

No Aplica

Este documento contiene información de propiedad de Inteligo IPH. Antes de utilizarlo, verifique que la versión esté vigente a fin de evitar su uso indebido. De ser éste un documento de uso confidencial, no podrá ser objeto de reproducción total o parcial, tratamiento informático ni transmisión de ninguna forma sin autorización previa de Inteligo IPH.

Versión 1.0

Fecha de aprobación: 13/01/2026 | Revisado por: Procesos y Calidad

Fecha de vigencia: 21/07/2025

Control de Cambios

Versión	Fecha de Aprobación	Autor del Cambio	Resumen del Cambio	Revisado por	Autor del Cambio
1	01/08/2025	Analista de Seguridad de la Información Oficial de seguridad de la información	Primera Versión	Oficial de seguridad de la información	Gerente de Riesgos
2	13/01/2026	Analista de Seguridad de la Información Oficial de seguridad de la información	Se agregaron y actualizaron los siguientes puntos: • Principios • Adecuación de Ley N° 31814 con lineamientos existentes	Oficial de seguridad de la información	Gerente de Riesgos

Este documento contiene información de propiedad de Inteligo IPH. Antes de utilizarlo, verifique que la versión esté vigente a fin de evitar su uso indebido. De ser éste un documento de uso confidencial, no podrá ser objeto de reproducción total o parcial, tratamiento informático ni transmisión de ninguna forma sin autorización previa de Inteligo IPH.

Versión 1.0

Fecha de aprobación: 13/01/2026 | Revisado por: Procesos y Calidad

Fecha de vigencia: 21/07/2025