ACEVAL
Academia Nacional de Evaluadores de México
11 Años

IA4People

# Guía Institucional para la Gobernanza y el Uso Responsable de la Inteligencia Artificial Generativa

**Autores: Alfredo Domínguez Díaz y Diana Yolanda Valadez Rovelo**

## Tabla de contenido

# Introducción

En el contexto actual de transformación digital, la Inteligencia Artificial (IA) representa una oportunidad sin precedentes para potenciar la eficiencia, la innovación y la calidad en la prestación de servicios institucionales. La organización reconoce el papel estratégico de estas tecnologías como motor de valor público y mejora continua. Sin embargo, el despliegue de soluciones de IA conlleva una responsabilidad ética ineludible. Por ello, la institución reafirma su compromiso con un uso seguro, transparente y responsable de la inteligencia artificial, priorizando siempre la protección de los derechos, la integridad de la información y la supervisión humana. Esta guía establece el marco de gobernanza necesario para asegurar que cada avance tecnológico se desarrolle bajo estándares de excelencia, alineándose con nuestros valores fundamentales y fortaleciendo la confianza ciudadana en nuestra gestión.

# Capítulo 1: Fundamentos y Alcance

## 1. Objeto

La presente guía tiene por objeto establecer los principios, criterios, roles, controles y lineamientos generales para la gobernanza, adopción, desarrollo, implementación, supervisión y uso responsable de la inteligencia artificial dentro de la institución.

Su propósito es asegurar que toda iniciativa relacionada con inteligencia artificial se desarrolle de forma alineada con la misión institucional, con las obligaciones legales y regulatorias aplicables, y con estándares de diligencia, transparencia, trazabilidad, seguridad, calidad y responsabilidad.

La guía busca, además, favorecer la generación de valor institucional mediante el uso de tecnologías de inteligencia artificial, sin comprometer los derechos de las personas, la confidencialidad de la información, la integridad de los procesos ni la confianza en la gestión institucional.

## 2. Alcance

Esta guía aplica a todas las áreas, dependencias, unidades, proyectos, equipos de trabajo, personas servidoras, contratistas, proveedores y terceros que desarrollen, adquieran, integren, configuren, administren o utilicen soluciones de inteligencia artificial en nombre de la institución, o dentro de procesos institucionales.

También aplica a los casos en los que la inteligencia artificial se emplee como herramienta de apoyo para tareas como redacción, clasificación, predicción, análisis, asistencia a la toma de decisiones, automatización de procesos, generación de contenido, atención de consultas, traducción, búsqueda, resumen, recomendación o monitoreo.

La presente guía será aplicable tanto a soluciones internas como a servicios proporcionados por terceros, incluyendo herramientas en la nube, servicios software como servicio, asistentes generativos, motores de análisis predictivo, sistemas de recomendación y cualquier otra tecnología que encaje en la definición institucional de inteligencia artificial.

# Capítulo 2: Marco Referencial y Taxonomía de la IA

## 3. Marco de referencia

La interpretación y aplicación de esta guía deberá realizarse en armonía con el marco jurídico vigente, la normativa interna aplicable y los instrumentos institucionales relacionados con seguridad de la información, protección de datos personales, gestión documental, control interno, gestión de riesgos, continuidad operativa, transparencia, ética, integridad y contratación.

Cuando corresponda, podrán tomarse como referencia estándares, marcos o buenas prácticas internacionales en materia de inteligencia artificial, incluyendo, entre otros, principios de gobernanza, gestión del riesgo, supervisión humana, explicabilidad, robustez, seguridad, privacidad, rendición de cuentas y mejora continua.

En caso de que existan instrumentos institucionales específicos sobre determinadas materias —por ejemplo, ciberseguridad, privacidad, gestión de datos, auditoría o compras—, estos deberán coordinarse con la presente guía para evitar contradicciones y asegurar consistencia normativa y operativa.

## 4. Definiciones

Para efectos de esta guía, se entenderá por inteligencia artificial el conjunto de sistemas, modelos, técnicas o herramientas capaces de realizar tareas que usualmente requieren capacidades cognitivas humanas, tales como reconocer patrones, generar texto o imágenes, clasificar información, predecir resultados, recomendar acciones, traducir contenido, detectar anomalías o asistir en la toma de decisiones.

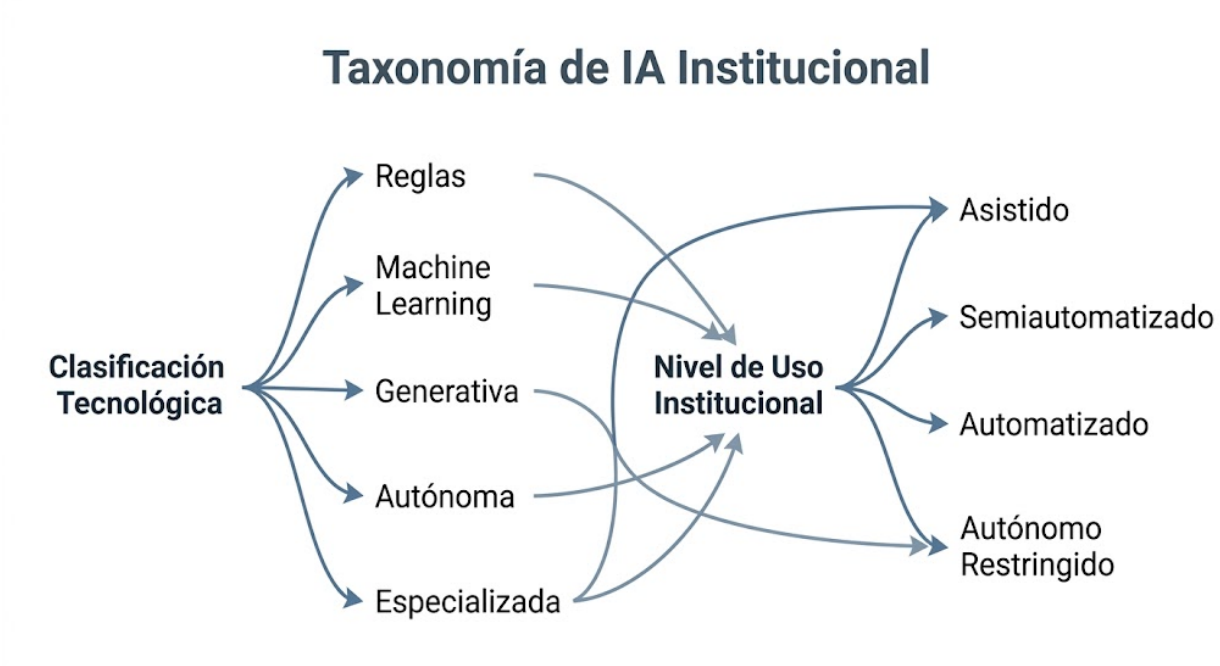


*Figura 1: Taxonomía de IA Institucional. Este diagrama integra la doble clasificación propuesta en la guía. A la izquierda, la clasificación por tipo tecnológico; a la derecha, la clasificación por nivel de uso institucional. La interconexión visual muestra cómo un mismo sistema técnico puede adoptarse bajo distintos modelos operativos.*

A fin de facilitar su gobernanza, la inteligencia artificial podrá clasificarse de dos formas complementarias:

### 4.1 Clasificación por tipo tecnológico

- **Sistemas basados en reglas o expertos:** operan mediante lógica predefinida, condiciones, reglas de decisión o conocimiento estructurado.
- **Sistemas predictivos o de aprendizaje automático:** utilizan datos para identificar patrones y generar predicciones, clasificaciones o recomendaciones.
- **Sistemas generativos:** producen contenido nuevo, como texto, imágenes, audio, código o combinaciones de estos, a partir de instrucciones o contexto.
- **Sistemas autónomos o semiautónomos:** ejecutan tareas o secuencias de acción con menor intervención humana directa, en mayor o menor medida.
- **Sistemas especializados de propósito limitado:** resuelven tareas concretas dentro de un dominio específico, con restricciones funcionales definidas.

### 4.2 Clasificación por nivel de uso institucional

- **Uso asistido:** la persona usuaria conserva el control principal y la IA actúa como apoyo puntual.
- **Uso semiautomatizado:** la IA ejecuta parte del proceso, pero requiere supervisión y validación humana significativa.
- **Uso automatizado:** la IA ejecuta tareas con mínima intervención humana, aunque bajo reglas predefinidas y controles institucionales.
- **Uso autónomo restringido:** la IA realiza acciones de mayor alcance bajo límites estrictos, aprobaciones específicas y supervisión reforzada.

Esta doble clasificación permitirá determinar el nivel de control, validación, documentación, monitoreo y aprobación aplicable a cada caso de uso.

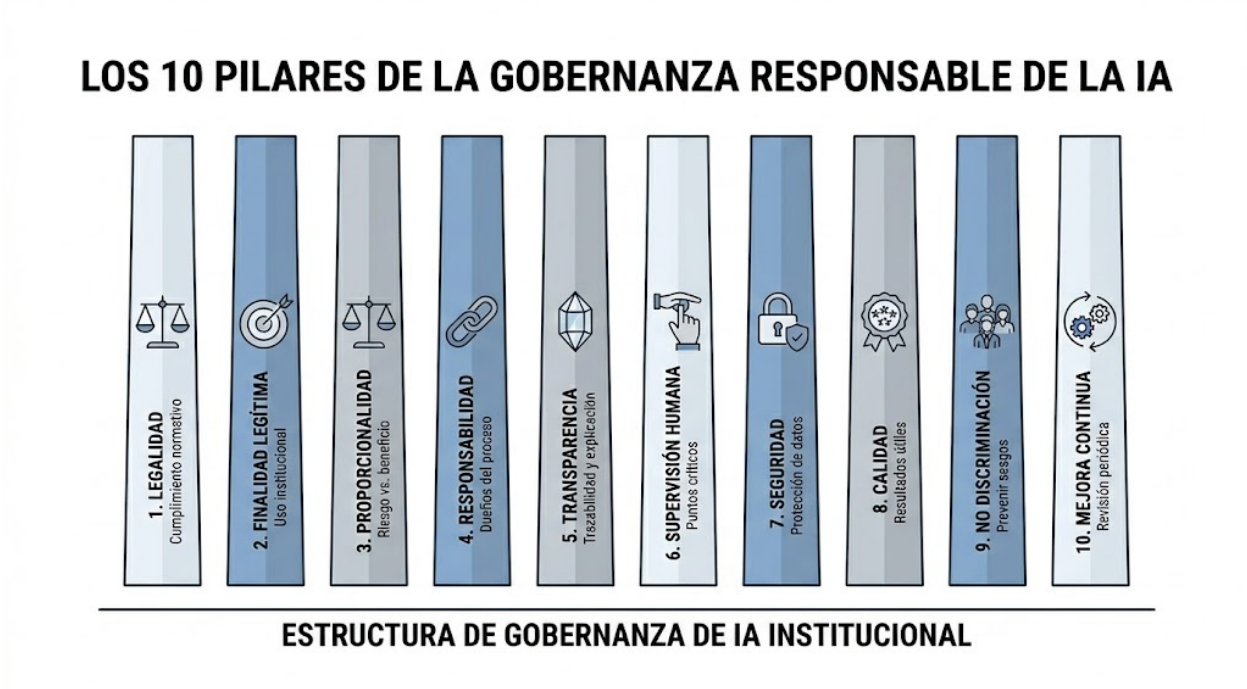


*Figura 2: Los 10 pilares de la Gobernanza. Este gráfico ilustra los diez principios fundamentales que sustentan el ecosistema de IA institucional: Legalidad, Finalidad legítima, Necesidad y proporcionalidad, Responsabilidad, Transparencia, Supervisión humana, Seguridad y confidencialidad, Calidad y confiabilidad, No discriminación y equidad, y Mejora continua. La disposición visual destaca la interdependencia de estos elementos para garantizar una gestión ética, segura y eficiente en todas las etapas del ciclo de vida de la IA.*

## 5. Principios rectores

El diseño, desarrollo, adquisición, implementación, operación y retiro de soluciones de inteligencia artificial deberán regirse por los siguientes principios:

- **5.1 Legalidad:** Toda actuación deberá ajustarse al marco normativo aplicable y a las políticas internas vigentes.
- **5.2 Finalidad legítima:** La inteligencia artificial solo deberá utilizarse para fines institucionales claros, justificados y compatibles con el mandato de la organización.
- **5.3 Necesidad y proporcionalidad:** El uso de inteligencia artificial y el nivel de control asociado deberán ser proporcionales al objetivo perseguido, al riesgo identificado y a la sensibilidad del proceso o de los datos involucrados.
- **5.4 Responsabilidad:** Toda solución o caso de uso deberá tener responsables claramente identificados para su diseño, aprobación, uso, seguimiento y eventual retiro.
- **5.5 Transparencia:** Cuando corresponda, deberá existir suficiente trazabilidad y capacidad de explicación sobre el uso de la inteligencia artificial, sus límites y sus efectos.
- **5.6 Supervisión humana:** La intervención humana deberá mantenerse en los puntos críticos del proceso, en especial cuando existan impactos relevantes sobre personas, derechos, decisiones o recursos.
- **5.7 Seguridad y confidencialidad:** La información institucional y personal deberá protegerse conforme a su clasificación, sensibilidad y requisitos de acceso.
- **5.8 Calidad y confiabilidad:** Los resultados generados o asistidos por inteligencia artificial deberán ser útiles, consistentes, verificables y adecuados para su propósito.
- **5.9 No discriminación y equidad:** Deberán adoptarse medidas razonables para prevenir sesgos, efectos discriminatorios o tratamientos injustos.
- **5.10 Mejora continua:** La institución deberá revisar y fortalecer sus controles, aprendizajes y prácticas de manera periódica.

# Capítulo 4: Modelo de Gobernanza y Responsabilidades

## 6. Gobierno institucional de la inteligencia artificial

La institución deberá establecer un esquema de gobernanza responsable de coordinar criterios, aprobar lineamientos, supervisar casos relevantes y promover el uso responsable de la inteligencia artificial.

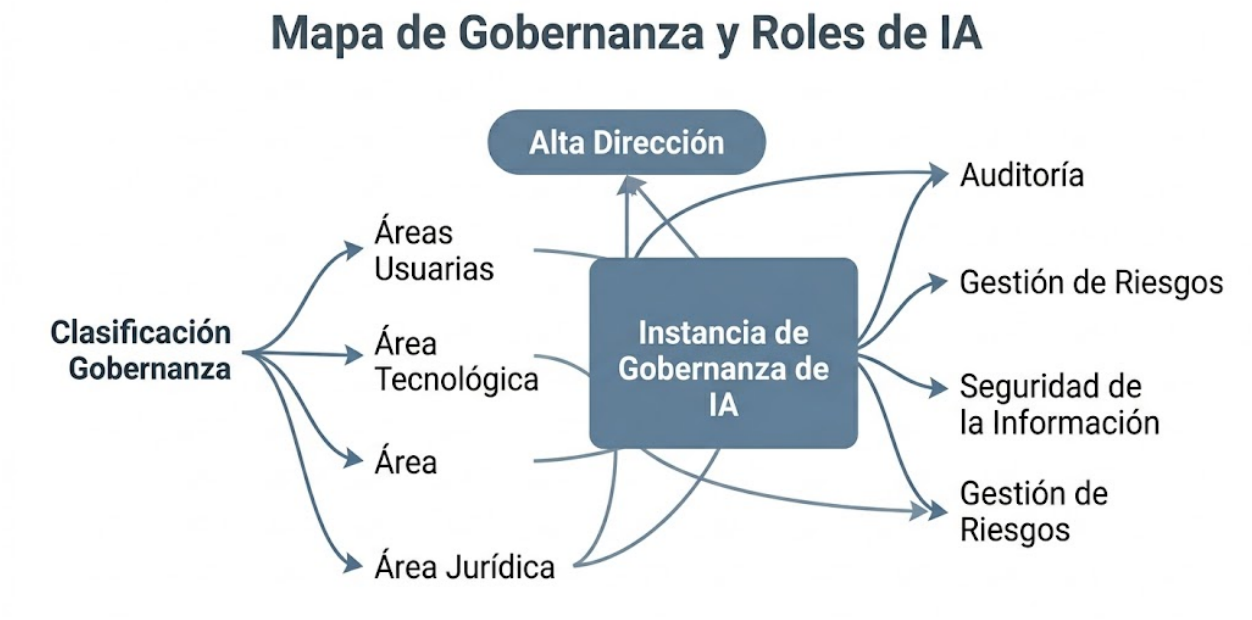


*Figura 3: Mapa de Gobernanza y Roles de IA. Este organigrama funcional ilustra el flujo de supervisión y la interconexión. La Alta Dirección define la estrategia, delegando en la Instancia de Gobernanza de IA la coordinación central. Esta instancia se articula con todas las áreas clave (satélites) para asegurar un cumplimiento integral y transversal.*

Dicho esquema podrá adoptar la forma de un comité, mesa técnica, instancia de coordinación o mecanismo equivalente, según la estructura institucional.

Como mínimo, la gobernanza deberá asegurar la articulación entre las áreas de dirección, tecnología, seguridad de la información, protección de datos, asesoría jurídica, gestión de riesgos, control interno y las unidades usuarias.

La gobernanza institucional deberá ser capaz de:

- definir criterios de admisibilidad para nuevos usos;
- evaluar riesgos antes de la adopción;
- determinar controles mínimos obligatorios;
- revisar incidentes o casos de desviación;
- proponer ajustes a la política o guía;
- documentar decisiones relevantes;
- y promover el aprendizaje institucional.

## 7. Roles y responsabilidades

La correcta implementación de esta guía exige la identificación clara de funciones y responsabilidades.

- **7.1 Alta dirección:** La alta dirección deberá promover la adopción responsable de inteligencia artificial, aprobar las orientaciones estratégicas, exigir el cumplimiento de la guía y asignar recursos cuando sea necesario.
- **7.2 Instancia de gobernanza de IA:** La instancia de gobernanza deberá coordinar criterios técnicos, operativos y de control; revisar usos de mayor riesgo; promover lineamientos; y documentar decisiones relevantes.
- **7.3 Áreas usuarias o dueñas del proceso:** Las unidades que proponen o utilizan inteligencia artificial deberán justificar la necesidad del caso de uso, definir el objetivo, identificar riesgos, asegurar la validación humana y verificar la calidad del resultado.
- **7.4 Área tecnológica:** El área tecnológica deberá evaluar la viabilidad técnica, la integración con sistemas institucionales, la seguridad, el soporte, la disponibilidad, la administración de accesos y la continuidad operativa.
- **7.5 Área jurídica o de cumplimiento:** Deberá revisar compatibilidad normativa, condiciones contractuales, obligaciones de uso, licenciamiento, confidencialidad, protección de datos, responsabilidad y otros aspectos de cumplimiento.
- **7.6 Área de seguridad de la información y privacidad:** Deberá evaluar los riesgos de confidencialidad, integridad, disponibilidad, tratamiento de datos personales, exposición de información sensible, fugas de datos y controles de protección.

- **7.7 Gestión de riesgos y control interno:** Deberá contribuir a la identificación, priorización, monitoreo y tratamiento de riesgos, así como a la verificación de la efectividad de los controles implementados.
- **7.8 Auditoría interna o control equivalente:** Deberá revisar evidencia, cumplimiento, trazabilidad y desempeño de los controles, cuando corresponda.
- **7.9 Proveedores y terceros:** Los proveedores deberán cumplir las cláusulas contractuales, requisitos de confidencialidad, seguridad, soporte, disponibilidad, reversibilidad, portabilidad y demás condiciones exigidas por la institución.

# Capítulo 5: Ciclo de Vida e Implementación

## 8. Ciclo de vida del uso de inteligencia artificial

La institución deberá gestionar toda solución de inteligencia artificial a lo largo de su ciclo de vida completo.


*Figura 4: Ciclo de Vida de la IA Institucional. Este diagrama circular ilustra el flujo secuencial y obligatorio de ocho etapas para cualquier solución de IA. Cada etapa cuenta con un icono minimalista descriptivo, subrayando que la gestión de la IA es un proceso continuo e iterativo, no un evento único.*

- **9.1 Identificación de la necesidad:** Toda iniciativa deberá responder a una necesidad real y documentada, asociada a un proceso, problema, oportunidad o mejora institucional.
- **9.2 Análisis de viabilidad:** Antes de iniciar la implementación, deberá verificarse si la solución es técnica, jurídica, operativa y económicamente viable.
- **9.3 Evaluación de riesgos:** Cada caso de uso deberá someterse a una evaluación de riesgos previa, proporcional a su criticidad.

- **9.4 Selección o desarrollo de la solución:** La institución deberá comparar alternativas, requerimientos, costos, riesgos, dependencia tecnológica y condiciones contractuales.
- **9.5 Pruebas y validación:** Antes de pasar a producción, la solución deberá probarse con datos representativos y criterios de aceptación claros.
- **9.6 Implementación:** La entrada en operación deberá realizarse con autorización, capacitación, controles y plan de seguimiento.
- **9.7 Monitoreo y mejora:** La solución deberá monitorearse para identificar errores, desvíos, sesgos, incidentes y oportunidades de mejora.
- **9.8 Retiro o sustitución:** Cuando la solución deje de ser necesaria, segura o conveniente, deberá desactivarse o sustituirse ordenadamente, preservando la información y la evidencia que corresponda.

## 9. Requisitos mínimos para adquisición o desarrollo

Toda solución de inteligencia artificial que se adquiera o desarrolle deberá cumplir, como mínimo, con requisitos técnicos, jurídicos y operativos previamente definidos por la institución.

Entre ellos, deberán considerarse los siguientes:

- propósito claramente definido;
- documentación técnica suficiente;
- controles de acceso y autenticación;
- capacidad de auditoría o registro;
- seguridad lógica y, cuando aplique, cifrado;
- condiciones de soporte y mantenimiento;
- reglas sobre ubicación y tratamiento de datos;
- reversibilidad o portabilidad;
- compatibilidad con sistemas institucionales;
- y cláusulas contractuales sobre confidencialidad, titularidad y uso de la información.

Cuando se trate de adquisiciones, la institución deberá asegurarse de que los requisitos de seguridad, privacidad, continuidad y salida del servicio estén debidamente incorporados.

# Capítulo 6: Gestión del Riesgo y Uso de Datos

## 10. Clasificación de usos de inteligencia artificial

Antes de adoptar una solución o iniciar un caso de uso, la institución deberá clasificarlo conforme a su criticidad, sensibilidad, impacto y nivel de automatización.

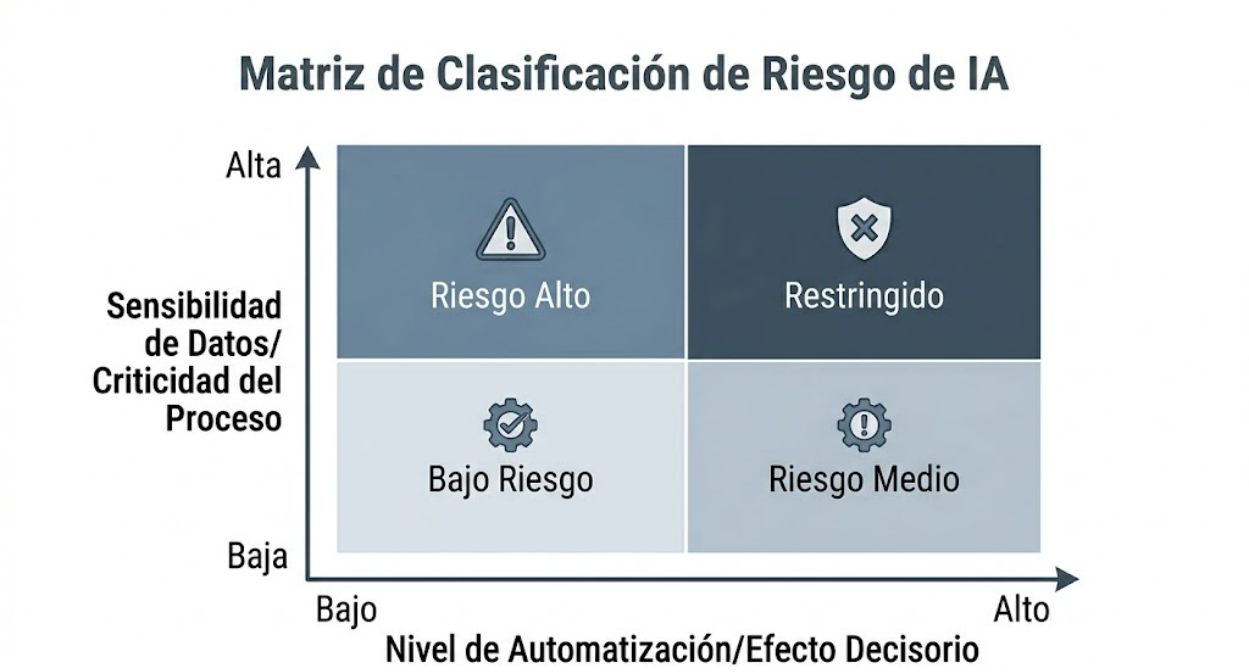


*Figura 5: Matriz de Clasificación de Riesgo de IA. Esta matriz cartesiana permite ubicar cualquier caso de uso de IA. El eje vertical mide la sensibilidad de los datos o la criticidad del proceso, y el eje horizontal el nivel de automatización o efecto decisorio. Las variaciones tonales de azul y gris indican visualmente el incremento de la criticidad, definiendo cuatro niveles de control obligatorios.*

- **8.1 Uso de bajo riesgo:** Corresponde a actividades de apoyo interno, sin manejo de información sensible, sin efectos decisorios relevantes y con alta posibilidad de revisión humana.
- **8.2 Uso de riesgo medio:** Corresponde a usos que implican automatización parcial, apoyo a procesos internos o manejo moderado de información, con necesidad de controles y validación humana definidos.

- **8.3 Uso de riesgo alto:** Corresponde a soluciones que influyen en decisiones importantes, tratan datos sensibles, impactan a personas o procesos críticos, o introducen dependencia significativa del modelo o del proveedor.
- **8.4 Uso restringido:** Corresponde a casos cuya criticidad exige autorizaciones expresas, controles reforzados y evaluación específica, o en los que el uso puede resultar no permitido por razones legales, éticas, técnicas o institucionales.

La clasificación deberá revisarse cada vez que cambien las condiciones del caso de uso, el tipo de dato, el proveedor, la finalidad o el contexto de operación.

## 11. Evaluación previa de riesgos

Toda adopción de inteligencia artificial deberá estar precedida por una evaluación de riesgos que considere, como mínimo:

- el tipo de información utilizada;
- la sensibilidad de los datos;
- la criticidad del proceso;
- el impacto potencial sobre personas o resultados;
- la dependencia del proveedor;
- la posibilidad de error, sesgo, alucinación o comportamiento no esperado;
- la explicabilidad de los resultados;
- la supervisión humana requerida;
- la continuidad operativa;
- la seguridad de la información;
- y la posibilidad de retiro o reversibilidad.

La evaluación deberá concluir si el uso es: permitido; permitido con condiciones; sujeto a autorización especial; o no permitido.

## 12. Uso de datos

El uso de datos en sistemas de inteligencia artificial deberá limitarse a la finalidad autorizada y observar los principios de minimización, proporcionalidad, licitud, confidencialidad y seguridad.

La institución deberá definir qué tipo de información puede utilizarse, bajo qué condiciones y con qué restricciones. En ningún caso deberán ingresarse datos personales, confidenciales, reservados o sensibles sin la evaluación y autorización requeridas, salvo que existan medidas técnicas y organizativas adecuadas, aprobadas institucionalmente.

Deberá prestarse especial atención a:

- datos personales y sensibles;
- información clasificada o reservada;
- información estratégica o crítica;
- secretos comerciales o contractuales;
- credenciales, claves o tokens;
- documentos internos no autorizados para difusión.

La institución podrá establecer listas de datos permitidos, restringidos y prohibidos.

# Capítulo 7: Supervisión, Operación y Seguridad

## 13. Supervisión humana

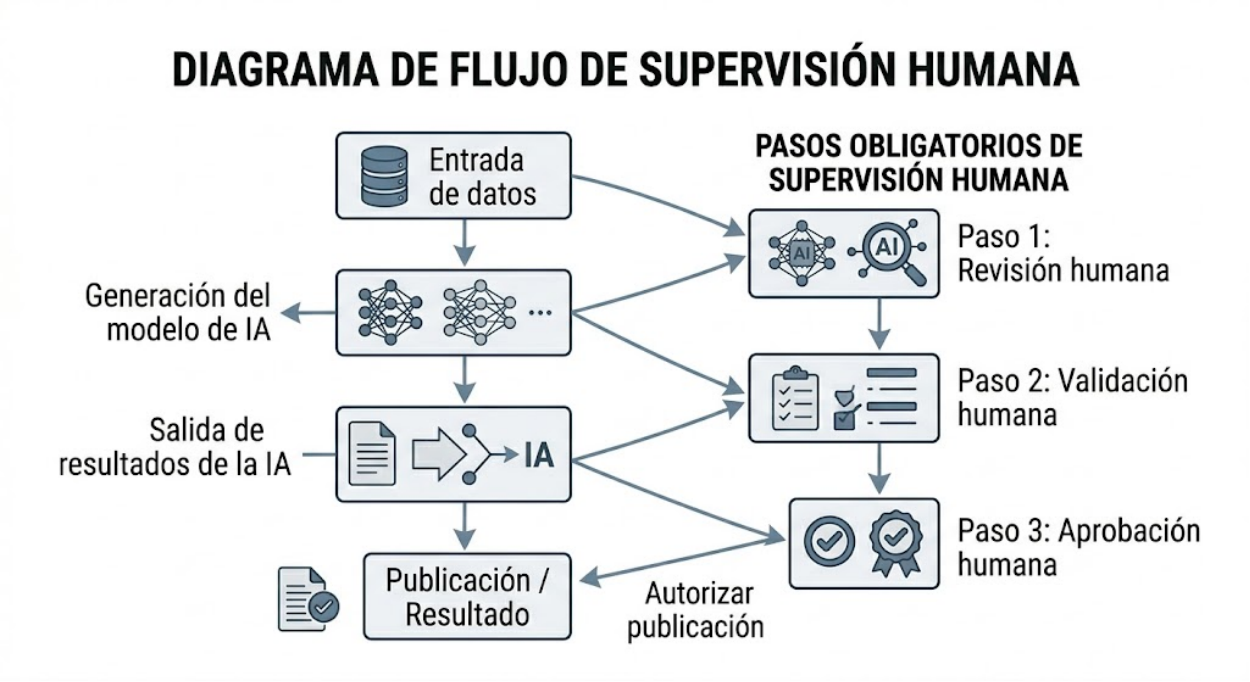


*Figura 8: Diagrama de flujo de supervición humana. Este organigrama funcional ilustra el flujo de supervisión y la interconexión entre lo que el modelo de IAG hace y como el humano se asegura de la calidad de las acciones del módelo.*

Todo uso de inteligencia artificial que pueda afectar decisiones, derechos, obligaciones, resultados relevantes, comunicaciones oficiales o procesos institucionales sensibles deberá contar con supervisión humana apropiada.

La supervisión humana podrá adoptar distintas formas, según el caso: revisión previa; validación posterior; aprobación por responsable autorizado; muestreo periódico; confirmación manual de resultados; corrección antes de su uso externo o institucional.

La supervisión no deberá ser meramente formal. Debe ser efectiva, capaz de detectar errores, omisiones, sesgos, inconsistencias o usos inapropiados.

## 14. Calidad, verificación y trazabilidad

Los resultados generados o asistidos por inteligencia artificial deberán verificarse antes de su uso final, especialmente si se utilizarán en documentos oficiales, análisis, recomendaciones, reportes, comunicaciones externas o decisiones operativas.

La verificación deberá considerar, según el caso: exactitud factual; consistencia lógica; completitud; pertinencia; alineación con el contexto institucional; y cumplimiento de formatos o estándares requeridos.

La institución deberá promover mecanismos de trazabilidad que permitan identificar, cuando sea aplicable:

- el caso de uso o proceso asociado;
- la persona responsable;
- la versión del sistema o modelo;
- la fecha de uso;
- la fuente o conjunto de datos utilizado;
- las validaciones ejecutadas;
- y los incidentes, errores o correcciones detectadas.

Cuando corresponda, deberá conservarse evidencia suficiente para permitir auditoría, revisión y aprendizaje institucional.

## 15. Reglas sobre prompts y uso operativo

Los prompts, instrucciones, consultas o entradas utilizadas para interactuar con sistemas de inteligencia artificial deberán diseñarse con claridad, precisión y control.

Como mínimo, deberán incluir o considerar: objetivo de la tarea; contexto necesario; alcance de la solicitud; restricciones o prohibiciones; formato esperado de salida; criterio de calidad; límites sobre uso de información; y requerimiento de revisión humana cuando aplique.

La institución podrá crear plantillas, patrones o estándares para el uso de prompts en funciones repetitivas, críticas o sensibles. Cuando se diseñen prompts institucionales, estos deberán someterse a pruebas con entradas representativas, revisión de resultados y documentación de la versión final.

## 16. Seguridad de la información y confidencialidad

El uso de inteligencia artificial deberá alinearse con la política institucional de seguridad de la información y con las obligaciones de confidencialidad aplicables.

Deberán evitarse prácticas que comprometan la seguridad o la privacidad, como por ejemplo:

- introducir información no autorizada en herramientas externas;
- compartir credenciales o secretos;
- utilizar cuentas personales para fines institucionales sin autorización;
- integrar herramientas no evaluadas;
- omitir controles de acceso;
- exportar información sensible sin validación;
- o desactivar mecanismos de protección.

La institución deberá aplicar, según corresponda, controles como segregación de ambientes, gestión de accesos, cifrado, monitoreo, registro de actividad, clasificación de información y revisión de permisos.

# Capítulo 8: Incidentes, Cultura y Mejora Continua

## 17. Gestión de incidentes y fallas

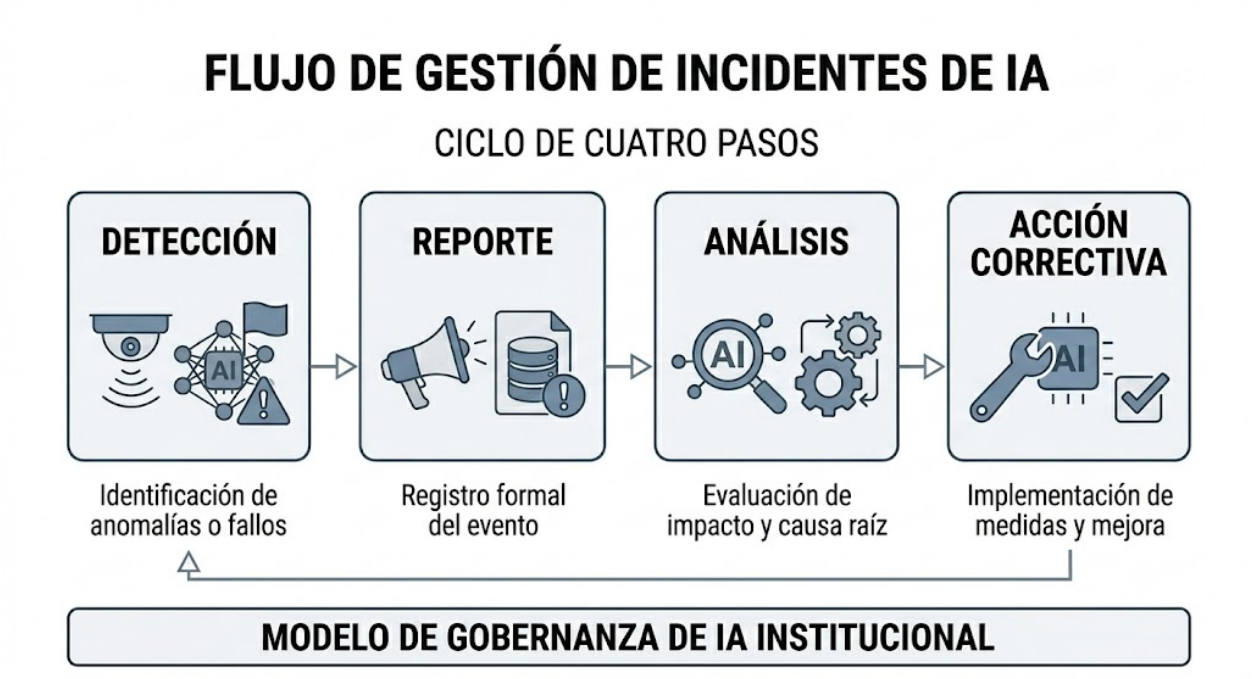


*Figura 9: Diagrama de flujo de gestión de incidentes de IA. Este diagrama muestra los 4 pasos prouestos para gestiónar incidentes con la IA en los flujos de trabajo, con el fin de mejorar las incidencias y los resultados.*

La institución deberá establecer mecanismos para reportar, registrar, analizar y atender incidentes relacionados con inteligencia artificial.

Se considerarán incidentes, entre otros: resultados erróneos con impacto relevante; generación de información falsa o engañosa; sesgos o discriminación; exposición de información confidencial; accesos no autorizados; fallas de disponibilidad; desviaciones respecto del uso aprobado; o comportamientos inesperados del sistema.

Todo incidente deberá analizarse para determinar su causa, impacto, medidas correctivas y eventuales acciones preventivas. Según la gravedad, podrá suspenderse temporalmente el uso de la solución mientras se corrigen las deficiencias detectadas.

## 18. Capacitación y cultura institucional

La adopción de inteligencia artificial deberá ir acompañada de acciones permanentes de capacitación, sensibilización y fortalecimiento de capacidades.

La formación institucional deberá abarcar, como mínimo: conceptos básicos de inteligencia artificial; oportunidades y límites de uso; riesgos frecuentes; validación de resultados; protección de datos y confidencialidad; uso responsable de prompts; sesgos y alucinaciones; supervisión humana; y responsabilidades individuales e institucionales.

La institución deberá promover una cultura de uso prudente, crítico, documentado y alineado con el interés institucional.

## 19. Seguimiento, revisión y mejora continua

La aplicación de esta guía deberá ser objeto de seguimiento periódico para verificar su efectividad, pertinencia y alineación con el entorno regulatorio y tecnológico.

La institución podrá revisar, entre otros aspectos: el inventario de casos de uso; la clasificación de riesgo; la efectividad de los controles; los incidentes ocurridos; los hallazgos de auditoría; las lecciones aprendidas; la necesidad de nuevas directrices o actualizaciones.

La mejora continua deberá traducirse en decisiones concretas, actualización de documentos, ajustes técnicos, capacitación adicional o redefinición de controles, según corresponda.

# Capítulo 9: Disposiciones Finales y Anexo

## 20. Disposiciones finales

La presente guía establece el marco institucional general para la gobernanza y el uso responsable de la inteligencia artificial dentro de la organización. Su aplicación deberá realizarse conforme a los principios, criterios, roles, controles y mecanismos aquí previstos, y en armonía con las demás políticas, lineamientos y disposiciones internas vigentes.

### 20.1 Carácter orientador y adaptabilidad

Esta guía deberá interpretarse como un instrumento de referencia institucional adaptable al contexto jurídico, técnico, operativo y organizacional de cada entidad. En consecuencia, su implementación podrá requerir ajustes, complementos o desarrollos específicos, siempre que no contradigan sus principios esenciales ni debiliten los controles mínimos de gobernanza, supervisión humana, trazabilidad, seguridad y responsabilidad.

### 20.2 Prelación normativa interna

En caso de existir normas internas, políticas, procedimientos o instructivos complementarios sobre temas relacionados con inteligencia artificial, seguridad de la información, protección de datos, gestión documental, riesgos, auditoría o cumplimiento, estos deberán armonizarse con la presente guía. Cuando exista conflicto entre disposiciones internas, deberá prevalecer la regla de mayor protección, mayor control o mayor rigor institucional.

### 20.3 Actualización de la guía

La presente guía deberá revisarse de manera periódica o cuando se produzca alguna de las siguientes circunstancias: cambios relevantes en el marco normativo aplicable; incorporación de nuevos tipos de sistemas o usos de IA; modificación sustantiva en el modelo de gobernanza; hallazgos de auditoría, incidentes o revisiones de riesgo; cambios en la estrategia institucional o en la madurez tecnológica; o aparición de

buenas prácticas que justifiquen su fortalecimiento.

### 20.4 Interpretación

La interpretación de esta guía corresponderá a la instancia competente designada por la institución, o a aquella unidad que tenga formalmente asignada la función de gobernanza, cumplimiento o control sobre la materia.

### 20.5 Entrada en vigor

La presente guía entrará en vigor en la fecha que determine la instancia competente al momento de su aprobación.

### 20.6 Derogación o sustitución

Con la entrada en vigor de esta guía, quedarán sin efecto aquellas disposiciones internas que se le opongan expresamente, o bien aquellas que hayan sido sustituidas de manera formal por instrumentos posteriores debidamente aprobados.

### 20.7 Revisión posterior

Sin perjuicio de su vigencia, la guía deberá permanecer abierta a revisión y mejora continua, de modo que pueda evolucionar conforme cambien las condiciones tecnológicas, regulatorias, organizacionales y operativas que inciden en el uso de inteligencia artificial.

### 20.8 Cláusula de responsabilidad institucional

La adopción de inteligencia artificial dentro de la organización no exime a las personas ni a las áreas competentes de sus deberes de diligencia, control, juicio profesional y observancia normativa. El uso de IA deberá entenderse como un apoyo a la gestión institucional, y no como sustituto de la responsabilidad humana.

### 20.9 Cierre

Con estas disposiciones, la institución reafirma su compromiso con una gobernanza de inteligencia artificial clara, transparente, responsable y sostenible, orientada a maximizar el valor institucional de estas tecnologías, sin comprometer la seguridad, la legalidad, la confianza ni la integridad de sus procesos.

## Anexo opcional. Criterios sugeridos para implementación inicial

Para facilitar la puesta en marcha de esta guía, la institución puede complementar su aplicación con los siguientes instrumentos:

- Inventario institucional de casos de uso de IA.
- Matriz de clasificación de riesgo.
- Formato de evaluación previa.
- Plantilla de autorización o aprobación.
- Guía interna de uso de prompts.
- Checklist de validación humana.
- Protocolo de incidentes.
- Cláusulas contractuales tipo para proveedores.
- Plan de capacitación.
- Calendario de revisión periódica.

Estos instrumentos podrán desarrollarse de manera progresiva, conforme la institución avance en madurez y adopción responsable de inteligencia artificial.