LA ÉTICA DE LA INTELIGENCIA ARTIFICIAL: UN DESAFÍO ESTRATÉGICO PARA EL SAIG

Resumen ejecutivo

La inteligencia artificial (IA) está transformando la gestión pública y generando oportunidades para mejorar la eficiencia, fortalecer el análisis de información y ofrecer servicios más oportunos a la ciudadanía. Sin embargo, su incorporación también introduce riesgos éticos, operacionales, legales y reputacionales que pueden afectar los derechos de las personas, la probidad, la transparencia y la confianza en las instituciones.

A nivel internacional, el desarrollo de la IA está acompañado por tres grandes tendencias: su acelerada adopción, el fortalecimiento de los marcos de gobernanza ética y la creciente necesidad de contar con controles y evaluaciones independientes. Estos avances muestran que los beneficios de la tecnología deben acompañarse de mecanismos que permitan identificar, gestionar y supervisar sus riesgos.

Chile forma parte de este proceso. La actualización de la Política Nacional de Inteligencia Artificial, las orientaciones para su utilización en el sector público, las recomendaciones sobre transparencia algorítmica y la discusión legislativa sobre la regulación de los sistemas de IA reflejan una creciente preocupación por promover una adopción responsable de estas tecnologías.

En este escenario, la creación del Servicio de Auditoría Interna de Gobierno (SAIG), mediante la Ley N° 21.769, adquiere especial relevancia. Su mandato de contribuir al fortalecimiento de la gobernanza, la gestión de riesgos y el control interno ofrece un marco institucional para incorporar los riesgos asociados a la inteligencia artificial en las actividades de aseguramiento y asesoramiento de la auditoría interna gubernamental.

El desafío es doble: preparar a los auditores internos para utilizar la inteligencia artificial de manera segura, efectiva y responsable, y desarrollar las capacidades necesarias para auditar los sistemas que la incorporan.

Este documento examina el contexto internacional y nacional, identifica seis dimensiones críticas de riesgo ético y propone líneas de acción que el SAIG podría impulsar, dentro de sus competencias, para fortalecer la capacidad de evaluación de la IA en los organismos públicos.

La conclusión central es que la ética de la inteligencia artificial no debe entenderse únicamente como una declaración de principios, sino como una dimensión concreta

de la gobernanza institucional, cuya aplicación debe poder demostrarse mediante responsabilidades definidas, controles efectivos y evidencia verificable.

1. La inteligencia artificial: una transformación que también desafía la confianza pública

La inteligencia artificial está cambiando la manera en que las instituciones trabajan, procesan información y toman decisiones. Herramientas que hace pocos años parecían lejanas hoy permiten analizar grandes volúmenes de datos, identificar patrones, automatizar tareas y apoyar procesos que antes requerían una intervención humana considerable.

Para el sector público, estas capacidades representan una oportunidad importante. La IA puede contribuir a mejorar la calidad de los servicios, optimizar recursos, anticipar necesidades y fortalecer la capacidad de respuesta de las instituciones.

Por ejemplo, puede apoyar la detección de inconsistencias en bases de datos, el análisis de solicitudes ciudadanas, la identificación de anomalías en procesos administrativos o la priorización de actividades de fiscalización. También puede facilitar tareas de análisis documental, elaboración de informes y búsqueda de información.

Sin embargo, la incorporación de estas tecnologías plantea interrogantes que van más allá de su desempeño técnico.

¿Qué ocurre si un sistema reproduce sesgos y perjudica injustificadamente a determinadas personas? ¿Cómo se explica una decisión administrativa cuando interviene un modelo algorítmico difícil de interpretar? ¿Quién responde si una herramienta automatizada entrega información incorrecta o ejecuta una acción no autorizada?

Estas preguntas adquieren especial relevancia en el Estado, donde las decisiones no solo deben ser eficientes, sino también ajustarse al ordenamiento jurídico, respetar los derechos fundamentales y responder al interés público.

Un sistema de IA puede funcionar correctamente desde una perspectiva técnica y, aun así, generar consecuencias injustificadas o incompatibles con los principios que orientan la función pública.

Por ello, la discusión sobre ética de la inteligencia artificial no puede reducirse a la calidad de los algoritmos ni a la seguridad informática. También debe considerar la forma en que las instituciones toman decisiones, asignan responsabilidades, gestionan riesgos y rinden cuentas.

El desafío no es únicamente incorporar tecnologías más avanzadas, sino asegurar que su utilización contribuya a una gestión pública confiable, transparente y responsable.

Esta realidad exige una mirada integral en la que la gobernanza, la gestión de riesgos y el control interno ocupen un lugar central.

2. Megatendencias globales: innovación, gobernanza y aseguramiento independiente

La evolución internacional de la inteligencia artificial permite identificar tres tendencias que están modificando la manera en que las organizaciones, tanto públicas como privadas, abordan su utilización.

2.1. La aceleración del desarrollo y adopción de la IA

La primera tendencia es la rapidez con que evolucionan las capacidades de los sistemas de inteligencia artificial.

El desarrollo de modelos generativos, sistemas multimodales y agentes capaces de ejecutar tareas con distintos niveles de autonomía está ampliando las posibilidades de aplicación de estas tecnologías.

Esta evolución ofrece beneficios, pero también genera nuevas formas de exposición al riesgo.

Una herramienta utilizada inicialmente para resumir documentos puede terminar apoyando decisiones administrativas. Un sistema diseñado para entregar recomendaciones puede incorporar posteriormente funciones que le permitan ejecutar acciones o interactuar con otros sistemas.

En consecuencia, el riesgo de una aplicación de IA no depende únicamente de su tecnología, sino también del propósito para el cual se utiliza, la información que procesa, su nivel de autonomía y las consecuencias de sus resultados.

Para las instituciones públicas, esto implica que la evaluación de riesgos no puede ser un ejercicio aislado realizado solo al momento de adquirir o implementar una herramienta. Debe mantenerse durante todo su ciclo de vida.

2.2. El fortalecimiento de la gobernanza ética

La segunda tendencia es el desarrollo de marcos de gobernanza destinados a orientar el uso responsable de la inteligencia artificial.

A nivel internacional, distintos organismos han promovido principios y metodologías relacionados con la equidad, la transparencia, la protección de datos, la responsabilidad y la supervisión humana.

Entre las referencias más relevantes se encuentran:

- La Recomendación de la UNESCO sobre la Ética de la Inteligencia Artificial, de 2021, que promueve un enfoque centrado en los derechos humanos y la dignidad de las personas.
- El Marco de Gestión de Riesgos de Inteligencia Artificial del NIST, conocido como AI RMF 1.0, que propone abordar los riesgos mediante funciones de gobernanza, identificación, medición y gestión.
- La norma ISO/IEC 42001:2023, que establece requisitos para implementar y mantener un sistema de gestión de inteligencia artificial.
- El Reglamento de Inteligencia Artificial de la Unión Europea, que adopta un enfoque regulatorio basado en riesgos y establece exigencias diferenciadas según las características y usos de los sistemas.

Estos instrumentos no tienen la misma naturaleza jurídica ni son automáticamente obligatorios para los organismos públicos chilenos. Sin embargo, ofrecen referencias técnicas y de gobernanza que pueden apoyar la identificación de riesgos y el diseño de controles.

Su principal contribución es demostrar que la ética de la IA requiere estructuras de responsabilidad, procesos de gestión y mecanismos de supervisión.

2.3. La creciente necesidad de evaluaciones independientes

La tercera tendencia es el reconocimiento de que los compromisos éticos y los mecanismos de autorregulación, por sí solos, no son suficientes para generar confianza.

Las organizaciones necesitan demostrar que sus sistemas funcionan de manera adecuada, que los riesgos están siendo gestionados y que existen controles capaces de prevenir, detectar y corregir desviaciones.

Esto supone disponer de documentación, registros, pruebas, indicadores y mecanismos de seguimiento.

También requiere evaluaciones realizadas con suficiente objetividad e independencia respecto de quienes desarrollan, adquieren, administran o utilizan los sistemas.

Aquí aparece un espacio especialmente relevante para la auditoría interna.

Su función no consiste en reemplazar la gestión institucional ni asumir la responsabilidad por el funcionamiento de los modelos. Su aporte está en proporcionar aseguramiento independiente y asesoramiento sobre la adecuación y efectividad de los procesos de gobernanza, gestión de riesgos y control.

La principal conclusión de estas megatendencias es que la ética de la IA debe pasar de los principios declarados a prácticas institucionales que puedan verificarse.

Para el sector público, esta transición es fundamental, porque la confianza ciudadana depende no solo de los resultados que entrega la tecnología, sino también de la capacidad del Estado para explicar y responder por su utilización.

3. Chile y la construcción de un marco de gobernanza para la inteligencia artificial

Chile ha avanzado en la definición de políticas, orientaciones e instrumentos destinados a promover el desarrollo y uso responsable de la inteligencia artificial.

Estos antecedentes constituyen una base importante para comprender cómo el Estado está abordando la tecnología y qué oportunidades se presentan para la auditoría interna gubernamental.

3.1. La Política Nacional de Inteligencia Artificial

Un referente central es la Política Nacional de Inteligencia Artificial, cuya actualización fue aprobada mediante el Decreto N° 12 del Ministerio de Ciencia, Tecnología, Conocimiento e Innovación, promulgado en abril de 2024 y publicado el 28 de enero de 2025.

La política establece un horizonte estratégico hasta 2031 y se estructura en tres ejes: factores habilitantes, desarrollo y adopción, y gobernanza y ética.

Este último resulta especialmente relevante para la gestión pública, porque reconoce la necesidad de que el desarrollo tecnológico se acompañe de resguardos orientados a proteger los derechos de las personas y promover una utilización responsable de la IA.

Desde la perspectiva institucional, la política contribuye a situar la inteligencia artificial como un asunto que involucra distintas dimensiones de la gestión del Estado.

No se trata solamente de adquirir herramientas o desarrollar soluciones tecnológicas. También supone contar con capacidades organizacionales, profesionales y de supervisión que permitan utilizarlas adecuadamente.

Para la auditoría interna, esta orientación tiene una consecuencia importante: los riesgos de IA deben considerarse dentro de los procesos de gobernanza, gestión de riesgos y control interno de las instituciones que la utilizan.

3.2. El Plan de Acción de la Política Nacional de IA

La política se complementa con un Plan de Acción que contempla iniciativas para avanzar en el desarrollo, adopción y gobernanza de la inteligencia artificial.

Este instrumento permite conectar los objetivos generales de política pública con acciones destinadas a fortalecer las capacidades del país.

Desde la perspectiva del SAIG, su importancia radica en que ofrece antecedentes para comprender las prioridades nacionales y anticipar ámbitos donde la incorporación de IA podría generar nuevas necesidades de control y evaluación.

No obstante, es necesario distinguir entre los compromisos de política pública, las medidas programáticas y las obligaciones específicas que resulten exigibles a cada institución.

Esta distinción es fundamental para evitar que una auditoría trate una recomendación o una iniciativa programática como si constituyera, por sí sola, una obligación legal.

3.3. Las directrices para el uso de IA en el sector público

En el ámbito de la Administración del Estado, destaca el Oficio Circular N° 711, de diciembre de 2023, que entrega recomendaciones para el uso de herramientas de inteligencia artificial en el sector público.

Sus orientaciones consideran materias como la utilización responsable de estas tecnologías, la transparencia y explicabilidad, la prevención de discriminaciones, la privacidad, la protección de datos y la capacitación de los funcionarios públicos.

Este documento es especialmente relevante porque acerca la discusión ética a situaciones concretas de la gestión institucional.

Por ejemplo, cuando un organismo utiliza herramientas generativas para analizar documentos, procesar información o apoyar tareas administrativas, necesita considerar qué datos incorpora, cómo verifica los resultados y quién supervisa su utilización.

Desde la perspectiva de auditoría interna, estas orientaciones pueden servir como referencia para examinar si las instituciones han definido criterios de uso, responsabilidades y medidas de control.

Sin embargo, su naturaleza de recomendaciones debe respetarse al establecer los criterios de evaluación.

3.4. Transparencia algorítmica y derecho a comprender las decisiones públicas

Otro antecedente importante son las recomendaciones del Consejo para la Transparencia sobre transparencia algorítmica.

Estas orientaciones ponen de relieve la necesidad de que la ciudadanía pueda conocer, en los términos que correspondan, la utilización de sistemas automatizados en procesos institucionales y comprender cómo estos intervienen en las decisiones públicas.

La transparencia algorítmica adquiere especial importancia cuando una herramienta influye en decisiones que afectan derechos, beneficios u otras situaciones relevantes para las personas.

En estos casos, la documentación técnica no siempre es suficiente. Las instituciones también deben contar con mecanismos que permitan explicar las decisiones de manera comprensible y responder adecuadamente ante consultas o reclamaciones.

Para la auditoría interna, esto supone examinar la trazabilidad de los sistemas, la disponibilidad de información, la documentación de las decisiones y los mecanismos institucionales de revisión.

3.5. Gobierno Digital y madurez institucional

Las orientaciones de Gobierno Digital, incluida la Guía Metodológica del Sistema de Transformación Digital 2026, también aportan antecedentes para evaluar cómo las instituciones incorporan nuevas tecnologías en sus procesos.

La madurez digital no depende únicamente de disponer de herramientas avanzadas. También requiere capacidades de gestión, seguridad, gobernanza y supervisión.

En materia de IA, esto implica considerar aspectos como la definición de responsabilidades, la evaluación de riesgos, la trazabilidad y los resguardos éticos.

Para el SAIG, estas referencias pueden contribuir al desarrollo de criterios de auditoría adaptados a las características y capacidades de cada organismo.

En conjunto, los instrumentos nacionales muestran que la inteligencia artificial está dejando de ser una materia exclusivamente tecnológica para convertirse en un componente relevante de la gobernanza institucional.

El desafío es lograr que estas orientaciones se traduzcan en prácticas concretas, controles adecuados y mecanismos de seguimiento que permitan demostrar su aplicación.

4. La discusión legislativa sobre inteligencia artificial: un escenario que exige anticipación

A los avances de la política pública se suma la discusión en el Congreso Nacional del proyecto de ley que busca regular los sistemas de inteligencia artificial.

La iniciativa corresponde a los boletines N° 15.869-19 y N° 16.821-19, refundidos, y se encuentra en segundo trámite constitucional en el Senado.

El 26 de octubre de 2026, la Comisión de Desafíos del Futuro, Ciencia, Tecnología e Innovación aprobó el proyecto en general y dispuso su paso a la Sala. Por tanto, a la fecha de este documento, la iniciativa continúa en tramitación y no constituye una ley vigente.

4.1. Los principales temas del debate

La discusión legislativa ha abordado cuestiones relacionadas con la clasificación de los sistemas de IA según sus riesgos, la protección de los derechos fundamentales, la transparencia, la supervisión humana y las responsabilidades de los actores involucrados.

Uno de los enfoques considerados durante la tramitación ha sido establecer exigencias diferenciadas según la criticidad de los sistemas y las consecuencias que puedan generar.

Esta aproximación resulta relevante para el sector público, porque no todas las aplicaciones de IA presentan los mismos riesgos.

Una herramienta que ayuda a ordenar documentos administrativos no tiene necesariamente el mismo impacto que un sistema utilizado para apoyar decisiones sobre beneficios sociales, fiscalizaciones o selección de personal.

Por ello, el análisis de riesgos debe considerar el propósito del sistema, los datos utilizados, el grado de autonomía y las consecuencias potenciales de sus resultados.

El debate también ha puesto de manifiesto la necesidad de encontrar un equilibrio entre promover la innovación y establecer resguardos adecuados.

Un marco excesivamente rígido podría dificultar la adopción de soluciones beneficiosas. Por el contrario, la ausencia de controles suficientes puede generar daños, afectar derechos y debilitar la confianza pública.

El desafío regulatorio consiste en establecer condiciones proporcionales a los riesgos, sin perder de vista el interés general.

4.2. Su importancia para la Administración del Estado

Aunque el proyecto todavía puede experimentar modificaciones, su discusión entrega una señal relevante para los organismos públicos.

La utilización de inteligencia artificial estará cada vez más vinculada con expectativas de gobernanza, transparencia, gestión de riesgos y rendición de cuentas.

En consecuencia, las instituciones que incorporen estas tecnologías deberían considerar desde ahora cómo identificar los sistemas que utilizan, evaluar su criticidad, documentar las decisiones y establecer responsabilidades.

Esto no implica anticipar como obligatorias disposiciones que aún se encuentran en discusión. Significa reconocer que los riesgos existen independientemente de la entrada en vigencia de una futura ley.

Un sistema que genera resultados discriminatorios, expone información personal o adopta decisiones sin supervisión adecuada puede producir consecuencias relevantes aun cuando no exista una regulación específica de IA.

4.3. Una oportunidad para el SAIG

Para el SAIG, la discusión legislativa representa una oportunidad de preparación institucional.

Desde sus competencias, puede contribuir a desarrollar orientaciones técnicas, metodologías y capacidades de auditoría que permitan evaluar los riesgos asociados a la IA y adaptarse oportunamente a los cambios normativos que finalmente se aprueben.

Esta preparación debería considerar tanto el marco jurídico vigente como las tendencias regulatorias y los estándares técnicos pertinentes.

La auditoría interna no necesita esperar a que exista una ley específica para comenzar a evaluar riesgos relacionados con transparencia, protección de datos, seguridad, probidad o responsabilidad institucional.

Estos aspectos ya forman parte de materias que pueden ser relevantes para la gobernanza, la gestión de riesgos y el control interno de los organismos públicos.

El valor estratégico del SAIG estará en contribuir a que la auditoría interna gubernamental desarrolle una capacidad preventiva, capaz de anticipar riesgos y acompañar responsablemente la transformación tecnológica del Estado.

5. La Ley N° 21.769 y el papel estratégico del SAIG

La creación del Servicio de Auditoría Interna de Gobierno mediante la Ley N° 21.769, publicada el 17 de octubre de 2025, representa un avance institucional para fortalecer la auditoría interna gubernamental.

La ley establece un servicio público de carácter técnico, con funciones orientadas a contribuir al fortalecimiento de la gobernanza, la gestión de riesgos y el control interno de los organismos comprendidos en su ámbito de competencia.

Este mandato adquiere una nueva dimensión frente a los desafíos que plantea la inteligencia artificial.

5.1. Un mandato que permite abordar riesgos emergentes

Aunque la Ley N° 21.769 no está diseñada específicamente para regular la IA, sus disposiciones proporcionan un marco institucional para abordar los riesgos asociados a estas tecnologías desde el ámbito de la auditoría interna.

Entre los elementos relevantes se encuentran la Política de Auditoría General de Gobierno, los lineamientos técnicos, los planes de auditoría interna, la coordinación de las actividades de auditoría y el fortalecimiento de las competencias profesionales.

Estas herramientas pueden contribuir a incorporar progresivamente los riesgos de IA en la planificación y ejecución de los trabajos de auditoría.

Por ejemplo, si una institución utiliza un sistema algorítmico para apoyar decisiones administrativas relevantes, la auditoría interna podría evaluar si existen responsables definidos, controles sobre los datos, procedimientos de validación y mecanismos de supervisión humana.

De esta manera, el uso de IA puede abordarse como parte de los riesgos institucionales, sin necesidad de crear una función de auditoría completamente separada.

5.2. La Política de Auditoría General de Gobierno

El artículo 5 de la Ley N° 21.769 contempla la elaboración de la Política de Auditoría General de Gobierno, que contiene lineamientos estratégicos en materias de auditoría interna, gobernanza, control interno y gestión de riesgos.

Este instrumento ofrece una oportunidad para considerar los riesgos tecnológicos emergentes, incluida la inteligencia artificial, dentro de las prioridades estratégicas de auditoría interna gubernamental.

Su eventual incorporación permitiría entregar una señal institucional sobre la importancia de evaluar los riesgos asociados a tecnologías que pueden influir en decisiones públicas.

Sin embargo, dicha incorporación debe realizarse mediante los procedimientos y competencias establecidos en la ley.

5.3. Los lineamientos técnicos y las metodologías comunes

La Ley N° 21.769 también contempla la función del SAIG de establecer lineamientos técnicos dentro de su ámbito de competencia.

Esto abre un espacio para desarrollar criterios y procedimientos que permitan abordar los riesgos de IA de manera consistente.

Entre las materias que podrían considerarse se encuentran la identificación de sistemas, la evaluación de criticidad, la gobernanza de datos, la transparencia algorítmica, la supervisión humana y la gestión de proveedores tecnológicos.

El objetivo sería proporcionar herramientas que faciliten el trabajo de los auditores internos y promuevan criterios comunes de evaluación.

Estas metodologías deberían ser proporcionales a los riesgos y suficientemente flexibles para adaptarse a las distintas realidades institucionales.

5.4. Coordinación y fortalecimiento de la Red de Auditoría Interna

Uno de los desafíos de la auditoría de IA es que requiere conocimientos que no siempre forman parte de las competencias tradicionales de los equipos.

La coordinación de la Red de Auditoría Interna puede contribuir a enfrentar esta brecha mediante capacitación, intercambio de experiencias y difusión de buenas prácticas.

También puede facilitar el desarrollo de procedimientos especializados y mecanismos de colaboración con profesionales de tecnología, seguridad de la información, protección de datos y gestión de riesgos.

Esta articulación resulta especialmente importante para evitar que cada institución deba desarrollar sus capacidades de manera aislada.

5.5. Respeto de las competencias institucionales

El papel del SAIG debe ejercerse respetando las responsabilidades de cada organismo sobre sus sistemas de IA y las atribuciones de los organismos reguladores y fiscalizadores.

En particular, el artículo 8 de la Ley N° 21.769 establece que el SAIG debe ejercer sus funciones en coordinación con la Contraloría General de la República y sin perjuicio de las facultades que corresponden a esta última.

Por ello, su contribución no consiste en certificar universalmente los sistemas de IA ni sustituir la responsabilidad de las instituciones sobre su funcionamiento.

Su aporte está en fortalecer la capacidad de la auditoría interna para proporcionar aseguramiento y asesoramiento sobre la adecuación y efectividad de los procesos de gobernanza, gestión de riesgos y control.

En este sentido, el SAIG puede convertirse en un actor relevante para promover una evaluación más consistente y preventiva de los riesgos de inteligencia artificial en la Administración del Estado.

6. Seis dimensiones críticas de los riesgos éticos de la inteligencia artificial

La ética de la inteligencia artificial suele asociarse con principios como equidad, transparencia, privacidad y responsabilidad. Sin embargo, para la auditoría interna el desafío consiste en transformar esos principios en criterios que permitan evaluar situaciones concretas.

Un riesgo ético puede manifestarse en una decisión administrativa injustificada, en la utilización indebida de información, en la ausencia de mecanismos de revisión o en la falta de claridad respecto de quién responde por los resultados de un sistema.

Para abordar estos desafíos, se proponen seis dimensiones de evaluación que pueden servir como referencia para el desarrollo de metodologías y procedimientos de auditoría interna gubernamental.

6.1. Equidad y no discriminación algorítmica

Los sistemas de IA aprenden o generan resultados a partir de datos, reglas y modelos que pueden contener sesgos. Cuando estos elementos no son adecuados, los resultados pueden reproducir desigualdades existentes o generar diferencias injustificadas entre personas o grupos.

En el sector público, este riesgo adquiere especial relevancia cuando la tecnología interviene en procesos como la asignación de beneficios sociales, la selección de personal, la priorización de fiscalizaciones o la identificación de situaciones que requieren intervención institucional.

Por ejemplo, un sistema que utiliza información histórica para priorizar solicitudes podría reproducir patrones de atención que han favorecido sistemáticamente a determinados grupos, sin que ello responda a criterios objetivos y legítimos.

La dificultad es que estos sesgos no siempre son evidentes. Un sistema puede mostrar un buen desempeño general y, al mismo tiempo, producir resultados desfavorables para determinados segmentos de la población.

Desde la perspectiva de auditoría interna, corresponde evaluar si la institución identifica estos riesgos, examina la calidad y representatividad de los datos, realiza pruebas de equidad cuando resultan pertinentes y dispone de mecanismos para detectar y corregir diferencias injustificadas.

La evaluación debe considerar también si las variables utilizadas son apropiadas para la finalidad institucional y si existen procedimientos para revisar los resultados cuestionados.

El objetivo no es exigir resultados idénticos en todas las situaciones, sino comprobar que las diferencias de tratamiento respondan a criterios legítimos, justificables y compatibles con el ordenamiento jurídico.

6.2. Transparencia y explicabilidad

La transparencia es un elemento esencial de la confianza pública. Cuando una decisión administrativa se apoya en inteligencia artificial, debe ser posible comprender el papel que tuvo la tecnología y disponer de antecedentes suficientes para justificar el resultado.

Esto no significa que todos los sistemas deban explicar cada operación matemática de sus modelos. Significa que la institución debe contar con un nivel de documentación, trazabilidad y explicación adecuado a los riesgos de su utilización.

Un problema aparece cuando los funcionarios aceptan recomendaciones automatizadas sin comprender sus limitaciones o cuando la institución no puede reconstruir los antecedentes que sustentaron una decisión.

Por ejemplo, si un sistema recomienda priorizar determinados casos para fiscalización, debería existir información suficiente para comprender los criterios utilizados y verificar que la decisión final tenga un fundamento adecuado.

La auditoría interna debe examinar la documentación de los sistemas, la trazabilidad de los resultados, los registros de intervención humana y la existencia de mecanismos para explicar y revisar las decisiones.

También debe considerar si la institución comunica de manera apropiada la utilización de sistemas automatizados cuando ello resulta exigible o necesario para resguardar la transparencia y los derechos de las personas.

La explicabilidad no es únicamente un atributo técnico. Es una condición que puede resultar indispensable para la rendición de cuentas.

6.3. Privacidad y protección de datos personales

La inteligencia artificial puede procesar grandes cantidades de información, incluida información personal y sensible.

Su utilización puede generar riesgos cuando los datos se recopilan sin una finalidad suficientemente definida, se comparten con terceros sin los resguardos correspondientes o se incorporan a herramientas tecnológicas que no ofrecen garantías adecuadas de protección.

Un ejemplo cotidiano es el uso de aplicaciones de IA generativa para resumir documentos que contienen antecedentes personales, información reservada o datos institucionales sensibles.

Aunque la tarea parezca simple, puede generar riesgos si el funcionario desconoce cómo se procesa, conserva o utiliza la información ingresada.

En Chile, esta dimensión debe examinarse considerando el régimen de protección de datos personales aplicable y su evolución normativa, incluida la Ley N° 21.719, que contempla una entrada en vigencia diferida para sus principales modificaciones.

La auditoría interna debe evaluar si existen fundamentos legítimos para el tratamiento de datos, si se respeta la finalidad definida, si se aplica el principio de minimización y si los accesos están debidamente controlados.

También corresponde revisar las condiciones contractuales con proveedores, las transferencias de información, los mecanismos de seguridad y los procedimientos de respuesta ante incidentes.

La protección de datos debe considerarse durante todo el ciclo de vida del sistema, desde su diseño o adquisición hasta su operación y retiro.

6.4. Responsabilidad y rendición de cuentas

Una de las preguntas centrales de la ética de IA es quién responde cuando un sistema produce resultados incorrectos o genera consecuencias perjudiciales.

En muchas instituciones, los sistemas tecnológicos involucran distintas unidades: áreas usuarias, equipos informáticos, proveedores, responsables de datos y autoridades que adoptan decisiones.

Si las funciones no están claramente definidas, puede resultar difícil determinar quién debe supervisar el sistema, corregir sus errores o responder ante una reclamación.

Esta situación puede agravarse cuando se utilizan servicios externos cuyos modelos y procesos internos no son completamente conocidos por la institución.

La auditoría interna debe verificar que existan estructuras de gobernanza y responsabilidades definidas para las distintas etapas del ciclo de vida de los sistemas.

Esto incluye la autorización de su utilización, la evaluación de riesgos, la validación de resultados, la supervisión operativa, la gestión de incidentes y los mecanismos de corrección.

También debe examinar si las decisiones relevantes quedan documentadas y si existen procedimientos para atender reclamaciones y determinar responsabilidades.

La inteligencia artificial puede apoyar la toma de decisiones, pero no debe convertirse en una forma de diluir la responsabilidad institucional.

6.5. Autonomía y supervisión humana

La evolución de la IA está permitiendo desarrollar sistemas que no solo generan información o recomendaciones, sino que también ejecutan tareas, interactúan con otras aplicaciones y realizan acciones con distintos grados de autonomía.

Estos avances, especialmente en el ámbito de los agentes de IA, amplían las posibilidades de automatización, pero también introducen riesgos adicionales.

Un sistema podría ejecutar acciones incorrectas, utilizar información no autorizada o continuar operando sin que sus responsables detecten oportunamente una desviación.

Por ello, la supervisión humana debe diseñarse de acuerdo con la criticidad de las decisiones y el nivel de autonomía del sistema.

No basta con establecer formalmente que existe un funcionario supervisor. Es necesario comprobar que dispone de información, atribuciones, tiempo y capacidades suficientes para intervenir de manera efectiva.

La auditoría interna debe evaluar los límites de autonomía, los mecanismos de autorización, las condiciones para la intervención humana y los procedimientos de suspensión o desconexión.

También debe examinar si los responsables pueden cuestionar, modificar o rechazar los resultados automatizados y si existen registros de las acciones ejecutadas por el sistema.

La supervisión humana debe ser una capacidad real de control, no simplemente una formalidad incorporada al procedimiento.

6.6. Seguridad, probidad y confiabilidad

Los sistemas de IA también están expuestos a riesgos relacionados con seguridad informática, integridad de los datos, manipulación de modelos y generación de resultados incorrectos.

En el ámbito de la IA generativa, pueden producirse respuestas plausibles pero falsas, referencias inexistentes o interpretaciones equivocadas de la información.

Asimismo, pueden surgir riesgos asociados a la utilización de herramientas no autorizadas, dependencia excesiva de proveedores, conflictos de interés o decisiones de adquisición insuficientemente fundamentadas.

En el sector público, estos riesgos adquieren especial importancia por su relación con la probidad, la continuidad de los servicios y la adecuada utilización de los recursos.

La auditoría interna debe examinar los controles de acceso, la seguridad de los sistemas, la integridad de los datos, la validación del desempeño, la gestión de proveedores y los procedimientos de respuesta ante incidentes.

También debe evaluar si existen controles para prevenir el uso de herramientas no autorizadas y verificar la calidad de los resultados antes de incorporarlos a decisiones institucionales.

La confiabilidad de un sistema no debe presumirse por su sofisticación tecnológica. Debe respaldarse mediante pruebas, seguimiento y mecanismos de control adecuados.

6.7. Una evaluación integrada y proporcional al riesgo

Estas seis dimensiones no deben analizarse de manera aislada.

Un problema de transparencia puede dificultar la detección de discriminaciones. La ausencia de responsables puede impedir corregir errores. Una supervisión humana insuficiente puede aumentar las consecuencias de fallas técnicas o de seguridad.

Por ello, la evaluación debe considerar el sistema en su conjunto y el contexto institucional en que se utiliza.

La criticidad puede determinarse considerando, entre otros factores, el impacto potencial sobre los derechos de las personas, la sensibilidad de los datos, el nivel de autonomía, la escala de utilización y las consecuencias de un error.

Cuanto mayor sea el riesgo, mayor debería ser la exigencia de documentación, validación, supervisión y control.

Este enfoque permite evitar dos extremos: aplicar controles insuficientes a sistemas críticos o imponer exigencias desproporcionadas a herramientas de bajo riesgo.

7. De los principios éticos a los controles verificables

Chile cuenta con antecedentes técnicos que pueden contribuir a transformar los principios de ética de IA en criterios concretos de evaluación.

Entre ellos destaca la Guía de Formulación Ética de Proyectos de Ciencia de Datos, desarrollada por la División de Gobierno Digital y la Universidad Adolfo Ibáñez, con participación de GobLab UAI.

Este documento ofrece orientaciones para identificar y abordar riesgos éticos y legales durante el desarrollo de proyectos que utilizan datos y modelos algorítmicos.

Su importancia para el SAIG radica en que puede servir como referencia nacional para construir procedimientos de auditoría que permitan evaluar cómo las instituciones gestionan estos riesgos.

Complementada con las Normas Globales de Auditoría Interna, ISO/IEC 42001, el marco del NIST y otras referencias pertinentes, puede contribuir al desarrollo de metodologías adaptadas al sector público.

7.1. Una distinción fundamental: declarar, implementar y demostrar

En la práctica, una institución puede encontrarse en tres situaciones diferentes.

La primera consiste en declarar su compromiso con el uso ético de IA mediante políticas, principios o protocolos.

La segunda supone implementar medidas concretas para gestionar los riesgos identificados.

La tercera implica disponer de evidencia suficiente para demostrar que esas medidas funcionan y producen los resultados esperados.

Desde la perspectiva de auditoría interna, estas situaciones no son equivalentes.

Una política puede estar bien redactada, pero ser desconocida por los funcionarios. Un procedimiento puede existir formalmente, pero no aplicarse. Un control puede estar diseñado adecuadamente, pero funcionar de manera irregular.

Por ello, la auditoría debe distinguir entre el diseño de los controles y su efectividad operativa.

7.2. Ejemplo de aplicación en un organismo público

Consideremos una institución que utiliza un sistema de IA para apoyar la priorización de solicitudes de beneficios.

Una evaluación limitada podría verificar que existe autorización para utilizar el sistema, que se dispone de un contrato con el proveedor y que se han definido procedimientos administrativos.

Sin embargo, una auditoría orientada a los riesgos éticos debería profundizar en otras preguntas.

¿Se evaluó si los datos utilizados pueden generar resultados discriminatorios? ¿Existen antecedentes que permitan comprender las recomendaciones del sistema? ¿Se han definido responsables de supervisar los resultados? ¿Qué ocurre si una persona cuestiona una decisión? ¿Se realizan pruebas periódicas para detectar errores o cambios en el desempeño?

Responder estas preguntas requiere revisar documentación, examinar registros, realizar pruebas y obtener evidencia sobre el funcionamiento de los controles.

Este ejemplo muestra cómo la auditoría interna puede aportar una mirada que va más allá del cumplimiento formal.

7.3. La importancia de la evidencia

La evaluación de los controles de IA puede requerir diferentes tipos de evidencia, según la naturaleza y criticidad del sistema.

Entre ellas se encuentran inventarios de sistemas, evaluaciones de riesgos, documentación técnica, registros de decisiones, pruebas de validación, resultados de monitoreo, contratos, informes de incidentes y antecedentes de supervisión humana.

No todas las instituciones necesitarán el mismo nivel de documentación ni las mismas pruebas.

Lo importante es que los controles sean proporcionales a los riesgos y que exista evidencia suficiente, pertinente y confiable para evaluar su funcionamiento.

El aporte de la auditoría interna consiste en pasar de la confianza basada en declaraciones a una confianza respaldada por evidencia.

8. La inteligencia artificial como parte del Universo de Auditoría

Uno de los primeros desafíos prácticos para la auditoría interna gubernamental es identificar dónde y cómo se está utilizando la inteligencia artificial.

En muchas instituciones, estas tecnologías pueden incorporarse de manera progresiva, a través de proyectos formales, servicios contratados, funcionalidades integradas en plataformas existentes o herramientas utilizadas directamente por los funcionarios.

Esto significa que el uso de IA no siempre estará identificado como un proceso independiente dentro del Universo de Auditoría.

Por ejemplo, una institución puede utilizar algoritmos en sus procesos de fiscalización, asistentes generativos en tareas administrativas y modelos predictivos en actividades de planificación.

Si estos usos no se identifican adecuadamente, sus riesgos podrían quedar fuera de la evaluación institucional.

8.1. Identificación de sistemas y procesos

Un primer paso consiste en promover que las instituciones identifiquen los sistemas de IA que utilizan, los procesos en que intervienen y los responsables de su operación.

Este inventario debería considerar, según corresponda, la finalidad de cada sistema, los datos utilizados, los proveedores involucrados, el nivel de autonomía y las consecuencias potenciales de sus resultados.

La información permitiría reconocer áreas de mayor exposición al riesgo y orientar la planificación de auditoría.

8.2. Incorporación a la planificación basada en riesgos

La existencia de IA no implica automáticamente que todos los sistemas deban auditarse con la misma prioridad.

La planificación debería considerar su criticidad y su relación con los objetivos institucionales.

Los sistemas que intervienen en decisiones relevantes para las personas utilizan información sensible o ejecutan acciones con autonomía significativa pueden requerir mayor atención.

Por el contrario, herramientas de apoyo administrativo de bajo impacto podrían evaluarse mediante procedimientos más simples o dentro de auditorías de procesos existentes.

Este enfoque permite asignar los recursos de auditoría de manera eficiente.

8.3. Integración con otras materias de auditoría

Los riesgos de IA no necesariamente requieren auditorías independientes en todos los casos.

Pueden incorporarse en trabajos relacionados con gestión de beneficios, contratación pública, seguridad de la información, protección de datos, continuidad operacional, gestión de proveedores o control de procesos administrativos.

Por ejemplo, una auditoría sobre contratación tecnológica podría incluir la revisión de cláusulas relativas al tratamiento de datos, responsabilidades del proveedor y condiciones de supervisión de sistemas de IA.

Del mismo modo, una auditoría sobre gestión de beneficios podría examinar los controles de los modelos utilizados para apoyar la selección o priorización de solicitudes.

La clave es integrar la inteligencia artificial a la evaluación de los riesgos institucionales, evitando tratarla como un fenómeno separado de la gestión pública.

9. El desafío de auditar sistemas de IA y utilizar IA en la auditoría interna

La transformación tecnológica plantea dos desafíos complementarios para los auditores internos.

El primero consiste en desarrollar capacidades para evaluar los sistemas de inteligencia artificial utilizados por las instituciones.

El segundo es incorporar estas tecnologías de manera responsable en el propio trabajo de auditoría.

Ambas tareas requieren conocimientos, metodologías y controles adecuados.

9.1. Auditar sistemas que incorporan IA

La auditoría de IA exige comprender aspectos que pueden no formar parte de la formación tradicional de todos los auditores.

Entre ellos se encuentran el ciclo de vida de los modelos, la calidad de los datos, las pruebas de desempeño, los sesgos algorítmicos, la supervisión humana y los riesgos de seguridad.

Sin embargo, esto no significa que cada auditor deba convertirse en especialista en programación o ciencia de datos.

Lo fundamental es desarrollar capacidades suficientes para reconocer riesgos, formular preguntas pertinentes, evaluar los controles y determinar cuándo se requiere apoyo especializado.

La participación de profesionales de tecnología, seguridad de la información, protección de datos y otras disciplinas puede resultar necesaria en auditorías de mayor complejidad.

9.2. Utilizar IA en el trabajo de auditoría

La inteligencia artificial también puede contribuir a modernizar las actividades de auditoría interna.

Entre sus posibles aplicaciones se encuentran el análisis de grandes volúmenes de información, la identificación de anomalías, la clasificación de documentos, la elaboración de borradores y el apoyo a la evaluación de riesgos.

Estas herramientas pueden mejorar la productividad y permitir que los auditores dediquen más tiempo al análisis y al juicio profesional.

No obstante, su utilización también introduce riesgos.

Un resultado generado por IA puede contener errores, omitir información relevante o presentar conclusiones sin sustento suficiente.

Asimismo, el ingreso de información institucional a plataformas externas puede generar riesgos de confidencialidad y protección de datos.

Por ello, el uso de IA en auditoría debe estar sujeto a criterios claros de autorización, seguridad, validación de resultados y supervisión profesional.

9.3. El juicio profesional sigue siendo esencial

La inteligencia artificial puede apoyar el trabajo de auditoría, pero no reemplaza el juicio profesional ni la responsabilidad del auditor sobre sus conclusiones.

Los resultados generados por estas herramientas deben ser examinados críticamente y contrastados con evidencia suficiente, pertinente y confiable.

Esto es especialmente importante cuando la IA se utiliza para identificar hallazgos, evaluar riesgos o elaborar conclusiones.

El auditor debe mantener el control sobre el proceso y comprender las limitaciones de las herramientas utilizadas.

La incorporación responsable de IA no consiste en automatizar el juicio profesional, sino en fortalecer las capacidades del auditor para realizar evaluaciones de mayor calidad.

10. Una agenda estratégica para el SAIG

El contexto internacional, las orientaciones nacionales y la evolución legislativa permiten identificar una agenda de trabajo que el SAIG podría considerar, dentro de

sus competencias y prioridades institucionales, para fortalecer la auditoría interna gubernamental frente a los riesgos de IA.

Esta agenda no supone crear nuevas obligaciones regulatorias ni asumir responsabilidades que corresponden a otros organismos. Su propósito es proponer ámbitos de desarrollo técnico y profesional que contribuyan a mejorar la capacidad de aseguramiento y asesoramiento.

10.1. Incorporar los riesgos de IA en las orientaciones de auditoría

Una primera línea de acción consiste en considerar los riesgos asociados a la inteligencia artificial en las metodologías y orientaciones técnicas de auditoría interna.

Esto permitiría entregar criterios comunes para identificar sistemas, evaluar su criticidad y examinar los controles institucionales.

Las orientaciones podrían contemplar las seis dimensiones de riesgo ético descritas en este documento y su relación con los procesos de gobernanza, gestión de riesgos y control interno.

10.2. Desarrollar una metodología de evaluación basada en riesgos

Una segunda línea consiste en promover metodologías que permitan evaluar los sistemas de IA de manera proporcional a su criticidad.

Estas metodologías podrían incluir criterios para determinar el impacto potencial sobre las personas, la sensibilidad de los datos, el nivel de autonomía, la dependencia de proveedores y la exposición a riesgos de seguridad.

También podrían establecer procedimientos para evaluar el diseño y funcionamiento de los controles.

El objetivo sería facilitar evaluaciones consistentes, sin imponer exigencias uniformes a sistemas que presentan riesgos muy diferentes.

10.3. Fortalecer las competencias de la Red de Auditoría Interna

Una tercera línea consiste en desarrollar capacidades profesionales para abordar los desafíos de IA.

Esto podría incluir programas de formación sobre gobernanza, ética, riesgos algorítmicos, protección de datos, seguridad y uso responsable de herramientas generativas.

La formación debería combinar conocimientos conceptuales con casos prácticos y procedimientos de auditoría.

También sería conveniente promover la colaboración entre auditores y especialistas de otras disciplinas.

10.4. Promover evaluaciones piloto

Una cuarta línea consiste en desarrollar experiencias piloto de auditoría sobre sistemas o procesos que utilizan IA.

Estas evaluaciones permitirían probar metodologías, identificar dificultades y generar aprendizajes que puedan compartirse con la Red de Auditoría Interna.

Los pilotos podrían concentrarse inicialmente en ámbitos donde existan sistemas identificables, riesgos relevantes y disponibilidad de evidencia.

La experiencia obtenida permitiría perfeccionar los procedimientos antes de promover su utilización más amplia.

10.5. Impulsar buenas prácticas de gobernanza y control

Una quinta línea consiste en difundir buenas prácticas que ayuden a las instituciones a fortalecer sus mecanismos de gestión de riesgos y control interno.

Entre ellas podrían considerarse inventarios de sistemas, evaluaciones de impacto, documentación de decisiones, controles de acceso, validación de resultados y mecanismos de supervisión humana.

Estas buenas prácticas deberían adaptarse al marco normativo aplicable y a las características de cada organismo.

10.6. Prepararse para la evolución normativa

Una sexta línea consiste en mantener seguimiento de los cambios legislativos y regulatorios relacionados con IA, protección de datos, ciberseguridad y transformación digital.

La eventual aprobación de una ley específica de IA podría introducir nuevas exigencias que deban ser consideradas en las metodologías de auditoría.

La preparación anticipada permitiría actualizar oportunamente los criterios de evaluación y fortalecer las competencias de los equipos.

10.7. Evaluar el uso responsable de IA en la propia auditoría

Finalmente, el SAIG podría promover orientaciones para la utilización segura y responsable de herramientas de IA en las actividades de auditoría interna.

Estas orientaciones deberían considerar la confidencialidad de la información, la validación de resultados, la trazabilidad del trabajo y la preservación del juicio profesional.

De esta manera, la auditoría interna podría aprovechar los beneficios de la tecnología sin comprometer la calidad, independencia y confiabilidad de sus evaluaciones.

En conjunto, estas líneas de acción permitirían avanzar hacia una auditoría interna gubernamental mejor preparada para enfrentar los desafíos de la inteligencia artificial.

11. Propuesta de implementación gradual: de la preparación al aseguramiento

Para llevar esta agenda a la práctica, resulta conveniente considerar una implementación progresiva, que permita desarrollar capacidades y obtener aprendizajes antes de extender las metodologías a toda la Red de Auditoría Interna.

Se propone una hoja de ruta referencial de cuatro etapas, cuya aplicación dependerá de las prioridades, recursos y decisiones institucionales del SAIG.

1. **Etapa 1. Diagnóstico y preparación**

Identificar los principales usos y riesgos de IA en la Administración del Estado, revisar las referencias normativas y técnicas, y determinar las brechas de competencias de los equipos de auditoría.

Resultado esperado: diagnóstico inicial y prioridades para el desarrollo metodológico.

2. **Etapa 2. Desarrollo de orientaciones y capacidades**

Elaborar criterios de evaluación, procedimientos referenciales y herramientas de apoyo, junto con actividades de capacitación para los auditores internos.

Resultado esperado: metodología inicial y equipos preparados para aplicarla.

3. **Etapa 3. Aplicación piloto y aprendizaje**

Realizar evaluaciones piloto en procesos institucionales que utilicen IA, documentar los resultados y ajustar los procedimientos según la experiencia obtenida.

Resultado esperado: metodologías validadas en casos prácticos y buenas prácticas compartidas.

4. **Etapa 4. Integración y mejora continua**

Promover la incorporación de los riesgos de IA en la planificación basada en riesgos, fortalecer el intercambio de experiencias y actualizar las orientaciones conforme evolucione la tecnología y el marco normativo.

Resultado esperado: una capacidad de evaluación progresivamente integrada al trabajo habitual de auditoría interna.

Esta hoja de ruta no pretende establecer plazos obligatorios ni sustituir la planificación institucional. Su propósito es mostrar que el desarrollo de capacidades de auditoría de IA puede abordarse de manera gradual, ordenada y proporcional a los riesgos.

El énfasis inicial debería estar en conocer dónde se utiliza la tecnología, comprender sus riesgos y disponer de criterios mínimos para evaluar los controles.

A medida que se consoliden las capacidades, será posible avanzar hacia evaluaciones más especializadas y una mayor integración de estos riesgos en la planificación de auditoría.

12. Propuesta de matriz de riesgos éticos y criterios de auditoría

Como complemento práctico del análisis, se presenta una matriz referencial que vincula las seis dimensiones éticas con posibles controles y evidencias de auditoría.

Dimensión	Controles institucionales a evaluar	Evidencia posible
Equidad y no discriminación	Validación de datos, pruebas de sesgos y procedimientos correctivos	Informes de pruebas, resultados desagregados, registros de correcciones
Transparencia y explicabilidad	Documentación de modelos, trazabilidad y explicación de decisiones	Fichas técnicas, registros de decisiones, procedimientos de revisión
Privacidad y datos personales	Finalidad del tratamiento, minimización, accesos y seguridad	Evaluaciones de riesgos, autorizaciones, registros de acceso y contratos
Responsabilidad y rendición de cuentas	Roles definidos, supervisión, gestión de	Matrices de responsabilidades, actas, registros e informes

	incidentes y reclamaciones	
Autonomía y supervisión humana	Límites de autonomía, autorizaciones y mecanismos de intervención	Configuraciones, registros de aprobación, pruebas de suspensión
Seguridad, probidad y confiabilidad	Seguridad técnica, validación de resultados y gestión de proveedores	Pruebas de seguridad, informes de desempeño, contratos y registros de incidentes

Esta matriz no constituye una norma ni un programa de auditoría obligatorio. Es una propuesta conceptual que puede adaptarse según el tipo de sistema, el marco jurídico aplicable y los objetivos de cada trabajo.

Su utilidad radica en mostrar cómo los principios éticos pueden traducirse en controles observables y evidencia concreta.

De esta manera, la auditoría interna puede evaluar no solo si la institución reconoce determinados riesgos, sino también si dispone de medidas adecuadas para gestionarlos.

13. Reflexión final: una oportunidad para fortalecer la confianza en el Estado

La inteligencia artificial ofrece oportunidades importantes para modernizar la gestión pública, mejorar los servicios y utilizar de manera más eficiente los recursos del Estado.

Sin embargo, su verdadero aporte no dependerá únicamente de la sofisticación de los sistemas ni de la rapidez con que se incorporen nuevas herramientas.

También dependerá de la capacidad de las instituciones para utilizarlas con responsabilidad, comprender sus limitaciones y demostrar que sus decisiones respetan los derechos de las personas y el interés público.

Un sistema puede ser técnicamente avanzado y entregar resultados en segundos, pero eso no garantiza, por sí solo, que sus decisiones sean justas, transparentes o confiables.

Por ello, la ética de la inteligencia artificial debe incorporarse como una dimensión estratégica de la gobernanza, la gestión de riesgos y el control interno del Estado.

La evolución internacional, la Política Nacional de Inteligencia Artificial, las directrices para el sector público y la discusión legislativa chilena muestran que estos desafíos están adquiriendo una importancia creciente.

En este contexto, la Ley N° 21.769 proporciona al SAIG un marco institucional para contribuir al fortalecimiento de la auditoría interna gubernamental frente a los riesgos de IA.

Su aporte no consiste en reemplazar a los organismos reguladores, fiscalizadores o responsables de la gestión tecnológica. Consiste en promover capacidades de aseguramiento y asesoramiento que permitan evaluar si las instituciones identifican sus riesgos, establecen controles adecuados y verifican su funcionamiento.

El desafío es doble.

Por una parte, preparar a los auditores internos para utilizar la inteligencia artificial de manera efectiva, segura y responsable en su propio trabajo.

Por otra, desarrollar las competencias, metodologías y herramientas necesarias para evaluar los sistemas de IA que se incorporan a los procesos de la Administración del Estado.

Ambas tareas son complementarias. Una auditoría interna que comprende la tecnología estará mejor preparada para aprovechar sus beneficios y, al mismo tiempo, reconocer sus riesgos.

En este camino, el SAIG tiene la oportunidad de contribuir a una transformación de la auditoría interna gubernamental, promoviendo criterios comunes, fortaleciendo las capacidades profesionales y favoreciendo evaluaciones independientes basadas en evidencia.

La discusión legislativa refuerza la importancia de esta preparación. Aunque el proyecto de ley sobre IA continúa en tramitación, los riesgos asociados a estas tecnologías ya forman parte de la realidad de las instituciones que las utilizan.

Por ello, la auditoría interna no debería limitarse a reaccionar ante futuras exigencias normativas. También puede aportar una mirada preventiva que ayude a anticipar riesgos, fortalecer controles y mejorar la calidad de las decisiones institucionales.

El verdadero desafío no es simplemente incorporar inteligencia artificial al Estado, sino asegurar que su utilización contribuya a una gestión pública más justa, transparente, segura y responsable.

Y es precisamente en ese propósito donde el SAIG puede realizar una contribución estratégica: ayudar a que las instituciones no solo declaren su compromiso con una inteligencia artificial ética, sino que también puedan demostrarlo mediante una gobernanza sólida, controles efectivos y evidencia verificable.

Porque, en definitiva, la confianza ciudadana no se construye únicamente con tecnología más avanzada, sino con instituciones capaces de utilizarla responsablemente y rendir cuentas por sus resultados.

14. Referencias normativas, institucionales y técnicas

Marco nacional

1. Ley N° 21.769. Crea el Servicio de Auditoría Interna de Gobierno. Publicada el 17 de octubre de 2025. Biblioteca del Congreso Nacional. Texto legal

2. Decreto N° 12, de 2024, del Ministerio de Ciencia, Tecnología, Conocimiento e Innovación. Aprueba la actualización de la Política Nacional de Inteligencia Artificial. Publicado el 28 de enero de 2025. Texto oficial

3. Ministerio de Ciencia, Tecnología, Conocimiento e Innovación. Plan de Acción de la Política Nacional de Inteligencia Artificial. Política y Plan de Acción

4. Oficio Circular N° 711, de diciembre de 2023. Lineamientos para el uso de herramientas de inteligencia artificial en el sector público. Documento PDF

5. Congreso Nacional de Chile. Proyecto de ley que regula los sistemas de inteligencia artificial, boletines N° 15.869-19 y N° 16.821-19, refundidos. En segundo trámite constitucional al 3 de noviembre de 2026. Tramitación legislativa

6. Consejo para la Transparencia. Recomendaciones sobre Transparencia Algorítmica, 2025. Recomendaciones

7. Secretaría de Gobierno Digital. Guía Metodológica del Sistema de Transformación Digital 2026. Guía metodológica

8. División de Gobierno Digital y Universidad Adolfo Ibáñez, con participación de GobLab UAI. Guía de Formulación Ética de Proyectos de Ciencia de Datos.

9. Ley N° 21.719. Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. Considerar sus disposiciones transitorias y calendario de entrada en vigencia.

10. Ley N° 21.663. Ley Marco de Ciberseguridad.

Referencias internacionales

11. UNESCO (2021). Recomendación sobre la Ética de la Inteligencia Artificial.

12. National Institute of Standards and Technology, NIST (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0).

13. ISO/IEC 42001:2023. Information Technology: Artificial Intelligence Management System.

14. Instituto de Auditores Internos, IIA (2024). Normas Globales de Auditoría Interna, vigentes desde enero de 2025.

15. Unión Europea (2024). Reglamento (UE) 2024/1689, por el que se establecen normas armonizadas en materia de inteligencia artificial.