

REF.: APRUEBA PROTOCOLO PARA EL USO
RESPONSABLE DE INTELIGENCIA ARTIFICIAL EN LA
BIBLIOTECA DEL CONGRESO NACIONAL.

RESOLUCIÓN N° 0414

VALPARAÍSO, 22 SEP 2026

VISTOS Y CONSIDERANDO:

1. El Acuerdo Primero del Acta N° 5 de fecha 05 de noviembre de 2025 de la Honorable Comisión de Biblioteca, que nombra en el cargo de Director a don Ignacio Andrés Rodríguez Álvarez.
2. Que, conforme con los incisos segundo, tercero y séptimo del artículo 2° de la ley N° 18.918, Orgánica Constitucional del Congreso Nacional y el inciso segundo del artículo 3 del Estatuto de Personal de la Biblioteca del Congreso Nacional, corresponde a su Director el ejercicio de facultades de jefe superior del servicio y, en tal calidad, tiene a su cargo la administración del personal y de los distintos servicios de la Biblioteca.
3. Que, la Biblioteca del Congreso Nacional en el cumplimiento de su misión institucional de apoyar a la comunidad parlamentaria mediante información, conocimiento y asesoría especializada, reconoce que las herramientas de inteligencia artificial (en adelante, IA) pueden contribuir al fortalecimiento de sus procesos de investigación, análisis, gestión documental y elaboración de productos y servicios institucionales..
4. Que, sin perjuicio de sus beneficios, el uso de IA genera riesgos que deben ser gestionados adecuadamente. Entre ellos, destacan la generación de información incorrecta o no verificable, la reproducción de sesgos, el tratamiento inadecuado de datos personales o información protegida, la falta de trazabilidad de ciertos procesos y la eventual afectación de la calidad, confiabilidad o integridad de los productos y servicios institucionales.
5. Que, corresponde al Director de la Biblioteca la administración de los servicios de la Biblioteca y, consecuentemente fijar las normas de acceso y de uso de las Herramientas de Inteligencia Artificial.
6. Que, en consecuencia, procede aprobar el protocolo para el uso responsable de inteligencia artificial de la Biblioteca del Congreso Nacional las condiciones de acceso.

En mérito de lo anterior,

RESUELVO:

PRIMERO. Apruébese el Protocolo para el Uso Responsable de Inteligencia Artificial en la Biblioteca del Congreso Nacional, cuyo texto es del siguiente tenor:

**Protocolo para el Uso Responsable de Inteligencia Artificial en la Biblioteca del
Congreso Nacional**

Capítulo I. Introducción y propósito

1. Contexto institucional del uso de IA en la Biblioteca

La Biblioteca del Congreso Nacional de Chile (en adelante la Biblioteca), en cumplimiento de su misión institucional de apoyar a la comunidad parlamentaria mediante información, conocimiento y asesoría especializada, reconoce que las herramientas de inteligencia artificial (en adelante, IA) pueden contribuir al fortalecimiento de sus procesos de investigación, análisis, gestión documental y elaboración de productos y servicios institucionales.

Asimismo, la utilización de estas tecnologías ofrece oportunidades para mejorar la eficiencia y eficacia de diversas tareas, ampliar capacidades de análisis y apoyar el trabajo técnico desarrollado por la institución.

Sin perjuicio de sus beneficios, el uso de IA genera riesgos que deben ser gestionados adecuadamente. Entre ellos, destacan la generación de información incorrecta o no verificable, la reproducción de sesgos, el tratamiento inadecuado de datos personales o información protegida, la falta de trazabilidad de ciertos procesos y la eventual afectación de la calidad, confiabilidad o integridad de los productos y servicios institucionales.

En atención a lo anterior, la Biblioteca estima necesario contar con criterios y orientaciones comunes que permitan promover un uso responsable de la IA, favoreciendo su adopción de manera segura, proporcional y coherente con los principios y obligaciones institucionales.

2. Objeto y alcance general del protocolo

El presente protocolo tiene por objeto establecer criterios generales, principios rectores, definiciones operativas y reglas mínimas para orientar el uso responsable de sistemas y herramientas de IA en la Biblioteca, garantizando la precisión, imparcialidad y seguridad de los productos y servicios elaborados en la institución.

En particular, el protocolo busca:

- a) Orientar el uso institucional de herramientas de IA.
- b) Promover una adopción responsable, flexible y proporcional al nivel de riesgo.
- c) Proteger la calidad, confiabilidad y trazabilidad de los productos institucionales.
- d) Resguardar los datos personales, la información reservada y secreta, la seguridad de la información y la confidencialidad institucional.
- e) Establecer criterios mínimos de supervisión humana, verificación de fuentes y responsabilidad funcionaria.
- f) Identificar usos que requieran evaluación o autorización previa, así como aquellos prohibidos o no autorizados.
- g) Favorecer el aprendizaje institucional y la actualización periódica de criterios, herramientas y buenas prácticas.

El protocolo será aplicable a todos los procesos, productos y servicios elaborados en la Biblioteca, así como a todas las personas que utilicen sistemas o herramientas de IA en el

marco de sus funciones. Esto comprende, según corresponda, a funcionarias y funcionarios, jefaturas, personas contratadas a honorarios, prestadores de servicios, consultores, proveedores u otros terceros que empleen dichas herramientas para fines institucionales o en el marco de una relación contractual, colaborativa o funcional con la Biblioteca.

La aplicación de este protocolo respecto de personas externas a la institución se entenderá sin perjuicio de las obligaciones que deban incorporarse en las respectivas bases de licitación, contratos y convenios que regulen su relación con la Biblioteca.

El alcance del protocolo comprenderá todas las herramientas tecnológicas sustentadas en IA. La aplicación del protocolo no dependerá de que la herramienta utilizada sea gratuita, institucional, personal, pública, privada, integrada en software de uso común, contratada por la institución o utilizada en proyectos piloto. Bastará que su uso tenga relación con funciones, productos, servicios, información o procesos institucionales de la Biblioteca.

3. Enfoque institucional

La Biblioteca adopta un enfoque de uso responsable, flexible y proporcional de la IA. Este enfoque supone reconocer que la IA puede contribuir al cumplimiento de la misión institucional, especialmente, cuando permite mejorar la eficacia y eficiencia, ampliar capacidades de análisis, simplificar tareas repetitivas, apoyar procesos documentales o generar insumos preliminares, entre otros aspectos.

Del mismo modo, implica reconocer que no todos los usos de IA presentan el mismo nivel de riesgo. Por ello, las exigencias de revisión, registro, autorización, transparencia y control deberán ser proporcionales al tipo de herramienta utilizada, al tipo de información tratada, a la finalidad del uso y al destino del producto o resultado generado.

En consecuencia, este protocolo distingue cuatro categorías de riesgo: bajo, medio, alto y extremo o prohibido. Las exigencias de revisión, registro, autorización y control serán proporcionales a cada categoría de acuerdo con lo estipulado en el capítulo V. Asimismo, este protocolo se concibe como un instrumento marco. Las orientaciones operativas, ejemplos, herramientas autorizadas, formularios, modelos de nota metodológica y matrices de riesgo podrán desarrollarse o actualizarse mediante anexos, guías breves u otros instrumentos complementarios, sin necesidad de modificar permanentemente el cuerpo principal del protocolo.

4. Relación con el marco institucional vigente

El presente protocolo se aplicará en armonía con el marco institucional vigente de la Biblioteca y con la legislación aplicable. Por consiguiente, sus disposiciones no sustituyen las obligaciones legales, reglamentarias, administrativas o internas vigentes, sino que las complementan mediante criterios generales para el uso responsable de herramientas de IA.

Capítulo II. Definiciones operativas

- a) **Sistema de inteligencia artificial (sistema IA):** Sistema tecnológico que, a partir de datos de entrada, genera resultados como predicciones, contenidos, clasificaciones, recomendaciones o decisiones que influyen en entornos físicos o digitales. Para efectos de este protocolo, comprende herramientas de IA generativa, sistemas de análisis documental, clasificadores, motores de búsqueda semántica y otras aplicaciones basadas en inteligencia artificial.
- b) **Inteligencia Artificial generativa (GenIA):** Categoría de sistemas de IA capaces de



generar contenido nuevo tales como texto, código, imágenes, audio u otros formatos a partir de instrucciones en lenguaje natural proporcionadas por la persona usuaria.

- c) **Herramienta de inteligencia artificial (Herramienta IA):** Para efectos de este protocolo se entenderá como aplicación, interfaz, servicio o componente de software basado en uno o más modelos de inteligencia artificial.
- d) **Modelo de lenguaje de gran escala (LLM):** Sistemas entrenados sobre grandes volúmenes de texto que pueden redactar, resumir, traducir, responder preguntas y apoyar análisis. Existen diversos sistemas, cada uno con capacidades diferentes, actualizaciones de conocimiento distinto y condiciones de uso diversos respecto de la confidencialidad de los datos.
- e) **Supervisión humana:** Revisión activa y responsable por parte de un funcionario o funcionaria competente antes de que cualquier resultado generado por IA sea comunicado, entregado o usado para tomar decisiones. No equivale a leer el texto por encima o a una revisión superficial: implica verificar los datos, evaluar la coherencia del análisis y asumir la responsabilidad del producto final.
- f) **Alucinación:** Fenómeno por el cual el sistema genera información que parece correcta, pero es inventada o inexacta, incluyendo citas bibliográficas, datos estadísticos o referencias legales que no existen. Es el riesgo más inmediato para el trabajo técnico-jurídico de la Biblioteca y el que más debe controlarse en los procesos de verificación.
- g) **Sesgo algorítmico:** Distorsión sistemática en los resultados de un sistema IA derivada de los datos con que fue entrenado. En análisis de contenido parlamentario o jurídico, estos sesgos pueden afectar la imparcialidad de los productos de la Biblioteca y producir efectos injustificados, discriminatorios o no representativos, derivados de los datos utilizados, del diseño del sistema o de las condiciones de su utilización.
- h) **Prompt o instrucción:** Texto o instrucción que la persona usuaria entrega a un sistema IA generativa para obtener una respuesta, contenido o resultado.
- i) **Riesgo:** Uso de un sistema de inteligencia artificial que pueda producir efectos adversos o consecuencias no deseadas, atendida la naturaleza de la información involucrada, la finalidad del uso, el grado de intervención humana y el impacto potencial sobre personas, procesos, productos o servicios institucionales.
- j) **Datos personales:** Los relativos a cualquier información concerniente a personas naturales, identificadas o identificables.
- k) **Datos sensibles:** Aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.
- l) **Información reservada:** Información cuyo acceso, divulgación o utilización se encuentra restringida conforme a la ley o a disposiciones institucionales vigentes. En general, esta información solo puede ser conocida en el ámbito de la unidad del órgano a que sea remitida.
- m) **Información secreta:** Información cuyo acceso, tratamiento o divulgación se encuentra prohibido o estrictamente restringido por disposición legal o institucional, debido a la especial sensibilidad de su contenido. En general, esta información sólo puede ser conocida por las autoridades o personas a las que vaya dirigida y por quienes deban intervenir en su estudio o resolución.
- n) **Fuentes de acceso público:** Todas aquellas bases de datos, cuyo acceso o consulta puede ser efectuada en forma lícita por cualquier persona, tales como el Diario Oficial, medios de comunicación o los registros públicos que disponga la ley.
- o) **Anonimización:** Procedimiento irreversible en virtud del cual un dato personal no puede vincularse o asociarse a una persona determinada, ni permitir su identificación,



por haberse destruido o eliminado el nexo con la información que vincula, asocia o identifica a esa persona. Un dato anonimizado deja de ser un dato personal.

- p) **Seudonimización:** Tratamiento de datos personales que se efectúa de manera tal que ya no puedan atribuirse a un titular sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona natural identificada o identificable.
- q) **Procedimiento de disociación de datos:** Todo tratamiento de datos personales de manera que la información que se obtenga no pueda asociarse a persona determinada o determinable.

Capítulo III. Principios rectores del uso de IA

- a) **Supervisión y responsabilidad humana irreducible:** El uso de sistemas de inteligencia artificial en la Biblioteca deberá mantenerse siempre bajo supervisión y responsabilidad humana efectiva. Ningún producto, análisis, recomendación o documento institucional, podrá basarse exclusivamente en resultados generados por sistemas de IA sin revisión, validación y control. La responsabilidad sobre el contenido final recaerá en quien elabore, firme o valide un producto institucional, con independencia de las herramientas tecnológicas utilizadas en su elaboración. Este principio no admite excepciones.
- b) **Imparcialidad y neutralidad institucional:** El uso de herramientas de IA deberá ser coherente con los principios o criterios de imparcialidad y pluralismo que orientan la función institucional de la Biblioteca. En consecuencia, deberán evitarse sesgos político-partidistas, representaciones parciales o enfoques que comprometan la neutralidad técnica de los productos y servicios institucionales.

La utilización de IA no podrá sustituir el criterio técnico requerido para resguardar el equilibrio analítico y el tratamiento riguroso de distintas perspectivas jurídicas, legislativas o doctrinarias.
- c) **Transparencia y trazabilidad:** El grado de transparencia y trazabilidad será proporcional al nivel de riesgo asociado, la finalidad del uso y el impacto del producto o servicio elaborado. El uso de sistemas de IA en procesos institucionales deberá ser trazable y susceptible de revisión posterior. Cuando su utilización tenga incidencia relevante en productos técnicos, análisis especializados o documentos dirigidos a usuarios internos o externos, la Biblioteca promoverá mecanismos proporcionales de documentación, registro o declaración del uso de IA.
- d) **Verificación de hechos y fuentes:** Todo contenido generado o asistido por IA deberá ser sometido a procesos de revisión y verificación antes de su incorporación a productos institucionales. Esto incluye, entre otros, datos cuantitativos, referencias normativas, citas bibliográficas, estadísticas y cualquier otra información susceptible de comprobación independiente. La información que no pueda ser razonablemente verificada no deberá incorporarse como contenido validado institucionalmente, es decir, la regla práctica es simple: si no se puede verificar, no se incluye. Asimismo, deberá respetarse la normativa aplicable en materia de propiedad intelectual.
- e) **Protección de datos e información reservada o secreta:** El uso de IA deberá respetar las obligaciones legales e institucionales sobre protección de datos personales, seguridad de la información, secreto y reserva institucional.
- f) **No discriminación:** La Biblioteca procurará prevenir que el uso de IA genere resultados discriminatorios o reproduzca sesgos injustificados basados en género, etnia, nacionalidad u otras categorías protegidas. Se debe considerar que los sistemas de IA



pueden reflejar sesgos presentes en sus datos de entrenamiento, por lo que los resultados generados deberán ser evaluados críticamente antes de su utilización institucional.

- g) **Proporcionalidad y pertinencia:** Las medidas de control, revisión, transparencia y supervisión aplicables al uso de IA deberán ser proporcionales al nivel de riesgo asociado, considerando el tipo de herramienta utilizada, la naturaleza de la información tratada, la finalidad del uso y el impacto del producto elaborado. El uso de la IA deberá ser pertinente con la naturaleza de la tarea y el perfil del requirente y en el proceso de trabajo en que se utiliza. Se evitará su empleo en contextos que demanden, predominantemente, sensibilidad institucional o política, o bien un criterio ético especializado.
- h) **Enfoque centrado en el proceso de trabajo:** La evaluación del riesgo del uso de IA considerará el flujo de trabajo completo en que se inserta la herramienta –la información que ingresa, su procesamiento, su verificación y el producto que se entrega– y no la herramienta de forma aislada. Una misma herramienta podrá representar distinto nivel de riesgo según el flujo en que se utilice.

Capítulo IV. Gestión de riesgos e incidentes

La Biblioteca deberá adoptar un enfoque de gestión de riesgos para el uso institucional de herramientas de inteligencia artificial, con el objeto de identificar, evaluar, prevenir, mitigar y monitorear proactivamente aquellos riesgos e incidentes que puedan afectar la legalidad, seguridad, confiabilidad, integridad, ética, transparencia o adecuado funcionamiento de sus procesos, productos y servicios.

La gestión de riesgos deberá aplicarse de manera proporcional al nivel de riesgo, complejidad e impacto institucional del uso de inteligencia artificial de que se trate, conforme a la clasificación establecida en el capítulo siguiente.

Para estos efectos, deberán considerarse, a lo menos, las siguientes dimensiones de riesgo:

- a) **Riesgo legal y de cumplimiento:** Riesgo de que el desarrollo, adquisición o uso de herramientas de inteligencia artificial infrinja normas legales, reglamentarias, contractuales o disposiciones internas aplicables a la Biblioteca.
- b) **Riesgo ético y de derechos fundamentales:** Riesgo de que el uso de herramientas de inteligencia artificial genere resultados discriminatorios, sesgados o incompatibles con los principios de igualdad, no discriminación, transparencia u otros derechos fundamentales.
- c) **Riesgo de privacidad y protección de datos:** Riesgo derivado del tratamiento inadecuado de datos personales, sensibles, confidenciales o sujetos a reserva legal, incluyendo su divulgación, pérdida o utilización no autorizada.
- d) **Riesgo de ciberseguridad y/o tecnológico:** Riesgo de afectación a la disponibilidad, integridad o confidencialidad de la información institucional, así como de interrupción, degradación o vulneración de sistemas y procesos producto del uso de herramientas de inteligencia artificial.
- e) **Riesgos operacionales de inexactitud de la información o alucinación:** Riesgo de generación de información incorrecta, incompleta, engañosa o carente de sustento verificable que pueda afectar la calidad de los productos, servicios o decisiones institucionales.
- f) **Riesgo de opacidad:** Riesgo derivado de la imposibilidad de comprender, justificar o auditar adecuadamente los resultados, recomendaciones o decisiones generadas por

una herramienta de inteligencia artificial.

La gestión y tratamiento de riesgos deberá considerar la metodología de gestión de riesgos que utiliza la Biblioteca denominada "Procedimiento de gestión y tratamiento de riesgos".

La gestión de riesgos deberá orientarse por los principios de prevención, proporcionalidad y mejora continua. En este marco, los riesgos deberán ser evaluados considerando tanto sus potenciales efectos adversos como las oportunidades que el uso responsable de herramientas de inteligencia artificial pueda generar para el cumplimiento de los objetivos institucionales.

Los incidentes reportados deberán ser analizados conforme a su naturaleza y gravedad, con el objeto de adoptar las medidas correctivas, preventivas o de mitigación que resulten procedentes.

Capítulo V. Clasificación de riesgos según tipo de uso

La utilización de herramientas de inteligencia artificial deberá clasificarse conforme al nivel de riesgo asociado al uso específico que se pretenda realizar.

La clasificación de riesgos prevista en el presente protocolo dependerá del uso específico, considerando la naturaleza de la información involucrada, la finalidad perseguida, el grado de intervención humana y el impacto potencial del resultado, y no del tipo de herramienta utilizada. En consecuencia, una misma herramienta de inteligencia artificial podrá presentar distintos niveles de riesgo según el contexto y forma en que sea utilizada.

Para estos efectos, se distinguen las siguientes categorías:

1. Riesgo bajo:

Corresponde a usos de inteligencia artificial destinados principalmente a tareas operativas, administrativas o de apoyo, respecto de las cuales la persona usuaria mantiene control directo sobre el proceso y el resultado generado y cuyo uso no produce efectos relevantes sobre productos o decisiones institucionales.

El nivel de riesgo bajo requerirá de una revisión del propio funcionario o funcionaria y/o de sus pares.

Para efectos orientadores, podrán considerarse los siguientes criterios:

- a) **Tipo de uso:** Apoyo administrativo, generación de ideas, elaboración de borradores, corrección de estilo, traducción de textos, organización de información, y otras tareas de uso personal.
- b) **Tipo de datos:** Información pública, información institucional ya publicada, documentos de trabajo sin información sensible, confidencial o secreta.
- c) **Finalidad del uso:** Mejorar la eficiencia operativa, apoyar tareas rutinarias y facilitar la elaboración preliminar de contenidos sujetos a revisión humana.
- d) **Destino final del producto:** Minutas, borradores, traducciones, notas de trabajo u otros productos de carácter preparatorio o interno.

2. Riesgo medio

Corresponde a usos de inteligencia artificial que contribuyen a la elaboración de productos institucionales destinados a usuarios internos o externos, o que involucran

información técnica especializada, requiriendo revisión y validación por parte de la jefatura correspondiente o de quien ésta determine.

El uso de riesgo medio requerirá siempre la validación de la jefatura directa y, eventualmente, de una instancia superior.

Para efectos orientadores, podrán considerarse los siguientes criterios:

- a) **Tipo de uso:** Elaboración de informes técnicos, generación de contenidos para difusión institucional, producción de material gráfico o audiovisual, análisis de información especializada, apoyo a la investigación y generación de código para herramientas internas.
- b) **Tipo de datos:** Información institucional, información técnica especializada, contenidos sujetos a derechos de autor o información que requiera validación experta.
- c) **Finalidad del uso:** Apoyar la investigación, la difusión institucional, la elaboración de productos especializados y la optimización de procesos internos.
- d) **Destino final del producto:** Informes, boletines, materiales de capacitación, contenidos de difusión institucional, aplicaciones o herramientas internas.

3. Riesgo alto

Corresponde a usos de inteligencia artificial que involucren información reservada o secreta; afecten procesos institucionales críticos; o, puedan generar impactos significativos sobre productos, servicios o decisiones institucionales. Estos usos deberán someterse a evaluación institucional previa y requerirán autorización expresa del Director para su implementación, conforme a los mecanismos de gobernanza establecidos en el presente protocolo.

Para efectos orientadores, podrán considerarse los siguientes criterios:

- a) **Tipo de uso:** Automatización de procesos institucionales críticos, generación de reportes mediante procesamiento automatizado de información, sistemas que apoyen procesos decisionales o que operen con un alto grado de autonomía.
- b) **Tipo de datos:** Datos personales, datos sensibles, entre otros.
- c) **Finalidad del uso:** Generación de productos o servicios críticos, apoyo a procesos de decisión, cumplimiento normativo o gestión de información de especial sensibilidad.
- d) **Destino final del producto:** Productos, servicios o resultados que puedan generar efectos relevantes sobre usuarios, procesos institucionales o decisiones de la Biblioteca.

4. Riesgo extremo o prohibido

Este nivel corresponde a usos de inteligencia artificial incompatibles con los principios, obligaciones y restricciones establecidos en el presente protocolo, cuyo desarrollo o utilización se encuentra prohibido en el ámbito institucional.

Se prohíbe el uso de herramientas de inteligencia artificial cuando involucren información secreta o reservada respecto de la cual exista prohibición legal, reglamentaria o institucional para su tratamiento mediante este tipo de tecnologías. Asimismo, se considerarán de riesgo extremo aquellos usos expresamente prohibidos por el presente protocolo o por las demás normas institucionales aplicables.

Para efectos orientadores, podrán considerarse como usos de riesgo extremo:

- a) El tratamiento de información cuyo uso mediante herramientas de inteligencia artificial se encuentre expresamente prohibido por la ley o por las normas institucionales aplicables.

- b) La utilización de herramientas de inteligencia artificial para eludir controles institucionales, mecanismos de revisión o procedimientos obligatorios establecidos por la Biblioteca.
- c) La generación o difusión deliberada de información falsa, engañosa o manipulada mediante sistemas de inteligencia artificial.
- d) La utilización de sistemas de inteligencia artificial en formas incompatibles con los principios de imparcialidad, no discriminación, protección de datos personales, confidencialidad o seguridad de la información establecidos en este protocolo.
- e) Los demás usos expresamente prohibidos por la normativa legal o institucional vigente.

Los usos clasificados como de riesgo extremo no podrán ser autorizados ni sometidos a medidas de mitigación, debiendo rechazarse o suspender su utilización.

Capítulo VI. Reglas operativas mínimas de uso

En concordancia con los principios rectores, el uso de sistemas y herramientas de IA en la Biblioteca deberá observar reglas operativas mínimas destinadas a resguardar la calidad, confiabilidad, trazabilidad y responsabilidad de los productos y servicios institucionales.

En este contexto, las reglas se aplicarán de manera proporcional al nivel de riesgo asociado al uso de IA, considerando, entre otros aspectos, el tipo de herramienta utilizada, la naturaleza de la información tratada, la finalidad del uso y el destino del producto o servicio generado.

En definitiva, el uso de IA en tareas institucionales deberá sujetarse, a lo menos, a las siguientes reglas operativas:

- a) **Responsabilidad individual del funcionario o funcionaria:** La responsabilidad sobre el producto o servicio final recaerá siempre en quien lo elabore, valide, firme, apruebe o comunique. En consecuencia, la utilización de IA no exime del deber de cumplimiento de las directrices y normas institucionales y legales vigentes.
- b) **Revisión humana de resultados:** Todo resultado generado o asistido por IA que sea utilizado en productos, servicios o procesos institucionales deberá ser revisado antes de su incorporación, comunicación o entrega. Para estos efectos, el proceso de revisión deberá considerar, al menos, la pertinencia del resultado, su coherencia con el encargo, la calidad de la información utilizada y la existencia de eventuales errores, omisiones, sesgos o afirmaciones no verificadas o no verificables.
- c) **Validación de fuentes y cita de IA:** Cuando el resultado generado por IA contenga referencias normativas, jurisprudencia, citas bibliográficas diversas, datos estadísticos, antecedentes históricos u otra información susceptible de comprobación o verificación, esta deberá ser siempre validada mediante fuentes primarias u oficiales. Las herramientas de IA no deberán ser citadas directamente como fuente jurídica, bibliográfica, documental u otra. En consecuencia, la información obtenida por IA que no pueda ser razonablemente verificada mediante fuentes idóneas no deberá incorporarse como contenido validado institucionalmente.
- d) **Uso proporcional al nivel de riesgo:** La aplicación de las reglas operativas previstas en este capítulo se realizará conforme a la clasificación de riesgos establecida en el Capítulo V.
- e) **Declaración de uso de IA cuando corresponda:** Deberán declararse los usos de IA que, atendida su naturaleza, incidencia en el producto final o nivel de riesgo, requieran transparencia adicional conforme a los criterios institucionales que se definan para estos

efectos.

- f) **Resguardo de información institucional:** No se deberá ingresar en herramientas de IA públicas, externas o no autorizadas por la institución, información reservada o confidencial, datos sensibles u otros antecedentes que puedan comprometer la seguridad, confidencialidad o integridad institucional de la Biblioteca.
- g) **Preferencia por herramientas institucionales o autorizadas:** Para el desarrollo de tareas institucionales deberá privilegiarse el uso de herramientas tecnológicas autorizadas o provistas por la Biblioteca, cuando estas existan. Asimismo, deberá evitarse el uso de herramientas de IA no autorizadas que puedan comprometer la seguridad, confidencialidad o integridad de la información institucional.
La autorización institucional de herramientas de IA se realizará conforme a las reglas de gobernanza establecidas en el Capítulo IX.
- h) **Consulta previa en caso de duda:** Cuando existan dudas razonables sobre el nivel de riesgo de un uso de IA, la naturaleza de la información involucrada, la procedencia o idoneidad de una herramienta tecnológica, la necesidad de declarar su uso o la aplicación de medidas de revisión se deberá consultar previamente a la jefatura respectiva o al Comité de Uso Responsable de Inteligencia Artificial conforme a los mecanismos establecidos en el Capítulo IX.

Capítulo VII. Protección de datos y confidencialidad

El uso de IA en relación con datos personales deberá respetar los principios establecidos en el artículo 3° de la Ley N° 19.628, modificada por la Ley N° 21.719 y, en particular, los principios de licitud y lealtad, de finalidad, de seguridad y de responsabilidad.

En caso de requerir la utilización de datos personales para el trabajo con una IA y, de ser posible, se deberá previamente evaluar la posibilidad de aplicar un proceso de anonimización o seudoanonimización de los datos personales.

Lo anterior no será necesario cuando los datos personales provengan de fuentes de acceso público.

Queda prohibido el uso de IA en relación con información de carácter secreta o reservada, sea que tal calificación haya sido realizada por la ley, o por el Director de la Biblioteca.

Capítulo VIII. Trazabilidad y registro institucional del uso de IA

La Biblioteca promoverá mecanismos razonables y proporcionales de trazabilidad y registro del uso de IA, con el objeto de facilitar la revisión posterior de procesos relevantes, fortalecer la responsabilidad administrativa e institucional, apoyar la gestión de riesgos y favorecer el aprendizaje organizacional.

Para estos efectos, deberán considerarse los siguientes criterios para la trazabilidad y registro institucional del uso de IA:

- a) **Criterio general de trazabilidad:** La trazabilidad del uso de IA deberá aplicarse de manera proporcional y razonable, atendiendo a la finalidad del uso, su nivel de riesgo, la información involucrada, la herramienta tecnológica utilizada y su eventual impacto en los productos, servicios, procesos o responsabilidades institucionales de la Biblioteca.
- b) **Oportunidad del registro:** La oportunidad del registro dependerá de la naturaleza del uso



- de IA. La evaluación de herramientas, integraciones o usos de alto riesgo deberá realizarse antes de su implementación; el registro de usos relevantes podrá efectuarse durante el proceso o antes de la entrega del producto o servicio; y los incidentes deberán registrarse una vez detectados.
- c) **Registro de herramientas de IA:** Se deberán mantener registros actualizados de las herramientas de IA adquiridas por la Biblioteca y de las autorizadas por ella.
 - d) **Registro de usos de riesgo alto:** Los usos de IA clasificados como de riesgo alto deberán registrarse conforme a los mecanismos de registro aprobados por el Director, a propuesta del Comité de Uso Responsable de Inteligencia Artificial. El registro se aplicará de manera proporcional, considerando la finalidad del uso, la herramienta utilizada, el tipo de información tratada y el destino del producto o servicio.
 - e) **Contenido mínimo del registro:** El registro deberá ser breve, proporcional y limitado a la información necesaria para permitir la trazabilidad del uso correspondiente, evitando incorporar antecedentes que no sean indispensables para la revisión, gestión de riesgos o aprendizaje institucional, salvo justificación institucional expresa.
 - f) **Inventario y aprendizaje institucional:** La institución implementará una estrategia de adquisición y capacitación continua en herramientas de IA, conforme a lo dispuesto en el capítulo X.

Capítulo IX. Gobernanza y supervisión

La gobernanza del uso de inteligencia artificial en la Biblioteca se organizará conforme a un enfoque proporcional al nivel de riesgo, complejidad e impacto institucional de cada uso, de acuerdo con la clasificación establecida en el Capítulo V del presente protocolo.

Su finalidad será asegurar la adecuada aplicación del presente protocolo, facilitar la gestión de riesgos, promover el uso responsable de herramientas de inteligencia artificial y establecer mecanismos claros de decisión, coordinación, consulta y supervisión institucional.

Para estos efectos, la gobernanza deberá permitir el uso responsable de IA en tareas de bajo riesgo; establecer mecanismos de revisión y validación para los usos de riesgo medio; someter a evaluación y autorización institucional previa los usos de riesgo alto; y excluir aquellos usos que, conforme al presente protocolo, sean calificados como prohibidos o de riesgo extremo.

1. Autoridad institucional

Corresponderá al Director de la Biblioteca la dirección superior y la adopción de las decisiones institucionales de carácter general relativas a la aplicación del presente protocolo, en el ámbito de sus atribuciones.

En particular, corresponderá al Director:

- a) Aprobar los criterios generales para la aplicación e interpretación institucional del presente protocolo.
- b) Autorizar, restringir, suspender o prohibir el uso institucional de herramientas de inteligencia artificial, cuando su nivel de riesgo, naturaleza, alcance o impacto institucional así lo requiera.
- c) Resolver sobre la autorización de los usos clasificados como de riesgo alto, previo informe del Comité de Uso Responsable de Inteligencia Artificial o de las unidades competentes, cuando corresponda.



- d) Aprobar las modificaciones del presente protocolo y aquellos anexos, guías, matrices de riesgo, criterios o instrumentos complementarios que establezcan reglas de aplicación general para la institución.
- e) Resolver las discrepancias que se produzcan entre jefaturas, unidades o el Comité de Uso Responsable de Inteligencia Artificial respecto de la interpretación o aplicación del presente protocolo.
- f) Determinar la integración, funcionamiento, dependencia y forma de coordinación de la instancia técnica prevista en este capítulo.

El ejercicio de estas atribuciones se entenderá sin perjuicio de las competencias y responsabilidades que correspondan a las jefaturas y demás unidades de la Biblioteca conforme a la normativa institucional vigente.

En caso de ausencia del Director, las atribuciones previstas en este capítulo serán ejercidas por quien lo subrogue conforme a las normas institucionales vigentes, sin perjuicio de la facultad del Director de delegar expresamente alguna de ellas conforme a dichas normas.

Cuando el uso de inteligencia artificial sometido a autorización o resolución conforme a este capítulo involucre directamente a la Dirección, la decisión corresponderá a quien lo subrogue conforme al párrafo anterior.

2. Instancia técnica de coordinación y apoyo consultivo

La Biblioteca contará con una instancia institucional de carácter técnico, asesor y consultivo, en adelante, "Comité de Uso Responsable de Inteligencia Artificial en la Biblioteca", destinada a apoyar al Director, a las jefaturas y a las distintas unidades de la Biblioteca en la aplicación del presente protocolo.

El Comité de Uso Responsable de Inteligencia Artificial en la Biblioteca tendrá, entre otras, las siguientes funciones:

- a) Canalizar y responder consultas técnicas relativas a la aplicación del protocolo.
- b) Asesorar en la clasificación de los niveles de riesgo asociados a los distintos usos de inteligencia artificial.
- c) Elaborar y proponer criterios técnicos comunes y buenas prácticas para el uso institucional de inteligencia artificial.
- d) Colaborar en la evaluación técnica de herramientas de inteligencia artificial y formular recomendaciones respecto de su autorización, restricción o utilización institucional.
- e) Emitir informes o recomendaciones respecto de los usos clasificados como de riesgo alto que deban ser sometidos a decisión del Director.
- f) Apoyar la implementación, mantención y actualización de los mecanismos institucionales de trazabilidad, registro e inventario del uso de herramientas de inteligencia artificial.
- g) Proponer al Director actualizaciones del protocolo y de sus anexos, guías, matrices de riesgo, instrumentos y herramientas complementarias.
- h) Promover buenas prácticas y apoyar las actividades de capacitación, seguimiento y aprendizaje institucional en materia de inteligencia artificial.
- i) Coordinar, cuando corresponda, la participación de las unidades especializadas de la Biblioteca en la evaluación de materias sometidas a su conocimiento.

El Comité de Uso Responsable de Inteligencia Artificial en la Biblioteca tiene un carácter exclusivamente técnico, asesor y consultivo, sin facultades resolutorias. Sus informes,



recomendaciones y propuestas no tendrán, en caso alguno, carácter vinculante para el Director, ni sustituirán, modificarán o limitarán las atribuciones que la ley y el Estatuto de la Biblioteca confieren a éste, a las jefaturas o a los demás departamentos o unidades de la Biblioteca.

3. Integración y funcionamiento de la instancia técnica de coordinación

El Comité de Uso Responsable de Inteligencia Artificial en la Biblioteca estará integrado por funcionarios y funcionarias de las distintas áreas de la Biblioteca cuyas competencias resulten pertinentes para las materias reguladas en este protocolo.

Su integración, funcionamiento, dependencia y forma de coordinación, así como la designación de quien ejerza su Secretaría Ejecutiva, serán determinados por el Director mediante el mecanismo institucional correspondiente.

El Comité sesionará, a lo menos, una vez por semestre. Asimismo, sesionará extraordinariamente cuando sea convocado por el Director, ya sea por iniciativa propia o a solicitud de la Secretaría Ejecutiva o de una jefatura de departamento. La solicitud deberá fundarse en el nivel de riesgo, la complejidad o el impacto institucional de la materia que se proponga someter al conocimiento del Comité.

La Secretaría Ejecutiva ejercerá la función permanente de coordinación del Comité, con el objeto de dar continuidad al trabajo institucional en esta materia, gestionar las consultas, coordinar las actividades de seguimiento y actualización, mantener los registros correspondientes y servir de enlace entre las áreas involucradas.

4. Rol de las jefaturas

Las jefaturas serán responsables de orientar y supervisar el uso responsable de inteligencia artificial en sus respectivas unidades, velando por la correcta aplicación del presente protocolo.

En particular, les corresponderá:

- a) Autorizar y validar los usos que, conforme al presente protocolo, correspondan a su nivel de competencia.
- b) Verificar que los productos elaborados con apoyo de inteligencia artificial sean sometidos a los mecanismos de revisión y validación que correspondan.
- c) Adoptar las medidas necesarias para asegurar el cumplimiento de las reglas relativas a protección de datos, confidencialidad, seguridad de la información, trazabilidad y verificación de fuentes.
- d) Derivar al Comité de Uso Responsable de Inteligencia Artificial aquellos casos que, por su nivel de riesgo, complejidad, novedad o impacto institucional, requieran evaluación o apoyo técnico adicional.
- e) Elevar al Director, directamente o a través del Comité de Uso Responsable de Inteligencia Artificial, los casos cuya resolución corresponda a dicha autoridad conforme al presente protocolo.

5. Participación de unidades competentes

Cuando la naturaleza, complejidad, especialidad técnica o nivel de riesgo de un determinado uso de inteligencia artificial lo requiera, el Director o el Comité de Uso Responsable de Inteligencia Artificial podrán solicitar la participación o informe de las unidades o referentes internos cuyas competencias resulten pertinentes.

La intervención de dichas unidades tendrá carácter técnico o asesor y se efectuará dentro del ámbito de sus respectivas competencias.

6. Evaluación y autorización de usos de riesgo alto

Todo uso clasificado como de riesgo alto deberá ser objeto de una evaluación institucional previa a su implementación.

El Comité de Uso Responsable de Inteligencia Artificial, con la participación de las unidades competentes cuando corresponda, analizará el uso propuesto y podrá emitir un informe que identifique sus riesgos, medidas de mitigación, condiciones de utilización y demás antecedentes relevantes para su evaluación.

La autorización para implementar un uso clasificado como de riesgo alto corresponderá al Director.

El Director podrá autorizarlo sujeto a condiciones o medidas específicas, disponer modificaciones antes de su implementación, suspender su utilización o rechazarlo cuando estime que los riesgos asociados no se encuentran adecuadamente controlados o resultan incompatibles con las obligaciones institucionales.

Los usos clasificados como de riesgo extremo o prohibido no podrán ser autorizados.

7. Evaluación e inventario de herramientas

El Comité de Uso Responsable de Inteligencia Artificial colaborará en la evaluación de las herramientas de inteligencia artificial que se utilicen o pretendan utilizar institucionalmente y mantendrá un inventario actualizado de aquellas que hayan sido evaluadas, autorizadas, restringidas o prohibidas.

La autorización, restricción, suspensión o prohibición de una herramienta para su uso institucional corresponderá al Director cuando, atendida su naturaleza, nivel de riesgo o impacto institucional, se requiera una decisión de carácter general.

Los criterios técnicos y procedimientos para la evaluación de herramientas serán propuestos por el Comité de Uso Responsable de Inteligencia Artificial y aprobados por el Director.

8. Canal institucional de consultas

El Comité de Uso Responsable de Inteligencia Artificial actuará como canal institucional de consulta para las jefaturas y unidades respecto de la aplicación del protocolo, la clasificación del nivel de riesgo de un determinado uso, la procedencia o idoneidad de una herramienta, la necesidad de revisión, registro o declaración del uso y la pertinencia de medidas de mitigación.

Las consultas podrán ser resueltas técnicamente por dicha instancia cuando se refieran a materias comprendidas dentro de los criterios previamente aprobados.

Cuando una consulta implique establecer un nuevo criterio institucional, autorizar un uso de riesgo alto, resolver una discrepancia relevante o adoptar una decisión que exceda las funciones consultivas y técnicas del Comité de Uso Responsable de Inteligencia Artificial, deberá ser elevada al Director para su resolución.

Capítulo X. Capacitación y desarrollo de competencias

La Biblioteca deberá promover el desarrollo progresivo de competencias para el uso seguro, responsable, ético y eficiente de herramientas de IA por parte de las personas sujetas al presente protocolo.



Las actividades de capacitación deberán considerar un enfoque práctico, continuo y orientado a la gestión de riesgos, con la finalidad de fortalecer las capacidades institucionales para utilizar herramientas de IA de manera segura, responsable y acorde con los principios establecidos en este protocolo.

La estrategia de capacitación se inspirará en los siguientes principios:

- a) **Obligatoriedad:** La Biblioteca establecerá actividades de capacitación obligatorias para las personas que utilicen o puedan utilizar herramientas de IA en el ejercicio de sus funciones. En su implementación podrá priorizar aquellas áreas que administren información sensible, secreta o reservada o sujeta a regímenes especiales de protección.
- b) **Enfoque basado en roles:** Las actividades de capacitación deberán considerar las funciones desempeñadas por las distintas personas usuarias, incorporando contenidos y casos prácticos relacionados con el uso cotidiano de herramientas de IA en el ámbito institucional.
- c) **Cultura de responsabilidad:** Las actividades de capacitación deberán promover el principio de supervisión humana, conforme al cual las personas usuarias mantienen la responsabilidad sobre los contenidos generados, utilizados, revisados o difundidos con apoyo de herramientas de IA.

Las actividades de capacitación deberán considerar, al menos, contenidos relacionados con:

- a) **Conceptos generales** sobre IA y sus principales aplicaciones.
- b) **Reglas institucionales** sobre el uso permitido, restringido y prohibido de herramientas de IA.
- c) **Gestión de riesgos** asociados al uso de herramientas IA incluyendo materias relativas a seguridad de la información, protección de datos personales, confidencialidad, sesgos, alucinaciones y verificación de contenidos.
- d) **Principios de integridad, transparencia, responsabilidad y supervisión humana** aplicables al uso de IA en el ámbito institucional.
- e) **Buenas prácticas** para el uso de herramientas de IA, incluyendo la formulación de instrucciones, validación de resultados y evaluación crítica de los contenidos generados.

Las actividades de capacitación deberán diseñarse considerando las funciones y necesidades de los distintos grupos de usuarios de la Biblioteca, priorizando aquellas áreas que, por la naturaleza de sus funciones, utilicen herramientas de IA o administren información reservada o secreta.

La participación en las actividades de capacitación que la Biblioteca defina como obligatorias constituirá un deber funcionario para las personas comprendidas en su ámbito de aplicación.

La Biblioteca podrá desarrollar actividades de capacitación, materiales de apoyo, guías prácticas, manuales, repositorios de buenas prácticas y otros instrumentos destinados a facilitar la aplicación del presente protocolo.

La experiencia obtenida a partir de las actividades de capacitación, consultas institucionales, incidentes reportados y evolución tecnológica deberá ser considerada para la actualización permanente de los contenidos formativos y de los materiales de apoyo asociados al presente protocolo.

SEGUNDO. Este Protocolo comenzarán a regir desde la fecha de la presente resolución.

TERCERO. **Publíquense** en la intranet institucional, en el sitio web de Transparencia Activa de la Biblioteca.

ANÓTESE, COMUNÍQUESE Y CÚMPLASE



IGNACIO ANDRÉS RODRÍGUEZ ÁLVAREZ
DIRECTOR
BIBLIOTECA DEL CONGRESO NACIONAL



Distribución

- Dirección
- Jefe Departamento de Administración y Finanzas
- Jefe Departamento de Servicios Legislativos y Documentales
- Jefe Departamento de Producción de Recursos de Información
- Jefe Departamento de Estudios y Extensión
- Jefe Área Asesoría Técnica Parlamentaria
- Jefe de Sistemas y Servicios de Información en Red
- Unidad de Fiscalía
- Unidad de Auditoría
- Unidad de Información Pública y Comunicaciones
- Oficina de Partes