PODER JUDICIAL DE LA FEDERACIÓN
SUPREMA CORTE DE JUSTICIA DE LA NACIÓN

VARIOS CT-VT/A-11-2025

INSTANCIAS VINCULADAS:

DIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN

PONENCIA DE LA MINISTRA ANA MARGARITA RÍOS FARJAT

7O0pFAPhp5ZXGk3O3AgvT/mpeD17QD6U12ylATkfKBY=

Ciudad de México. Resolución del Comité de Transparencia de la Suprema Corte de Justicia de la Nación, correspondiente al veintitrés de abril de dos mil veinticinco.

A N T E C E D E N T E S:

PRIMERO. Solicitud de información. El dieciocho de marzo de dos mil veinticinco, se recibió la solicitud registrada en la Plataforma Nacional de Transparencia con el folio 330030525000445, en la que se pidió, en la modalidad de copia simple, lo siguiente:

> *"Solicito se me proporcione información sobre el sistema, aplicación, herramienta o proceso electrónico de Inteligencia Artificial (IA) implementado por el Poder Judicial / Tribunal Superior de Justicia de ** (sic) *denominado '***'* (sic)*, cualquier otro sistema de inteligencia artificial, cualquier otro sistema experto o cualquier sistema de automatización que permita:*
>
> **Gestión de procesos*
> **Gestión de documentos*
> **Generación de documentos*
> **Gestión de recursos informáticos*
> **Gestión de recursos financieros*
> **Análisis predictivo de casos*
> **Generación de resúmenes de expedientes*
> **Automatización de notificaciones*
> **Cálculo de prestaciones*
> **Cálculo de indemnizaciones*
> **Ciberseguridad*

A. Aspectos Técnicos:
1. Nombre y versión de la herramienta, aplicación, sistema o proceso de IA.
2. Tipo de IA utilizada, por ejemplo, 'Aprendizaje automático, procesamiento del lenguaje natural, redes neuronales, sistemas expertos').
3. Descripción de las funciones específicas que realiza la herramienta: (Ej. 'Análisis predictivo de casos, generación de resúmenes de expedientes, automatización de notificaciones, cálculo de indemnizaciones laborales').
4. Algoritmos utilizados: (Ej. 'Regresión lineal, árboles de decisión, redes neuronales convolucionales').
5. Lenguajes de programación y tecnologías utilizadas en el desarrollo: (Ej. 'Python, Java, TensorFlow, PyTorch').
6. Arquitectura del sistema: (Ej. 'Sistema centralizado, sistema distribuido, basado en la nube').
7. Datos de entrenamiento utilizados para la IA: (Ej. 'Base de datos de expedientes judiciales, legislación vigente').
8. Proceso de validación y pruebas de la herramienta: (Ej. 'Metodología utilizada para asegurar la precisión y confiabilidad de la IA').
9. Medidas de seguridad implementadas para proteger la información: (Ej. 'Cifrado de datos, controles de acceso').
10. Capacidad de auditoría del sistema: (Ej. 'Registros de actividad, trazabilidad de las decisiones').

B. Aspectos Presupuestales:
1. Costo de adquisición o desarrollo de la herramienta: (Desglosado si es posible).
2. Costo de mantenimiento y actualización: (Anual o periódico).
3. Fuente de financiamiento: (Ej. 'Presupuesto del tribunal, fondos federales, donaciones').
4. Contratos con proveedores: (En caso de haberlos, solicitar una versión pública o resumida).

C. Aspectos de Funcionamiento y Administración:
1. Criterios de selección e implementación de la herramienta: (Justificación de su uso).
2. Personal encargado de la operación y mantenimiento de la herramienta: (Número y perfil; sin nombres).
3. Procedimientos de uso de la herramienta por parte de los funcionarios judiciales: (Manuales o guías).
4. Impacto de la herramienta en la eficiencia y tiempos de resolución de casos: (Estadísticas o estudios).
5. Mecanismos de evaluación del desempeño de la herramienta: (Indicadores clave de rendimiento).
6. Políticas de privacidad y protección de datos personales relacionadas con el uso de la IA:
(Cumplimiento con la normatividad vigente).
7. Mecanismos de atención a quejas o errores en el funcionamiento de la IA: (Protocolos de actuación).
8. Transparencia en el uso de la IA en los procesos judiciales: (Información pública disponible para las partes)."

7O0pFAPhp5ZXGk3O3AgvT/mpeD17QD6U12ylATkfKBY=

SEGUNDO. Acuerdo de admisión de la solicitud. En acuerdo de diecinueve de marzo de dos mil veinticinco, la Unidad General de Transparencia y Sistematización de la Información Judicial (Unidad General de Transparencia), por conducto del Subdirector General de Transparencia y Acceso a la Información, una vez analizados la naturaleza y contenido de la solicitud, con fundamento en los artículos 123 y 124, de la Ley General de Transparencia y Acceso a la Información Pública (Ley General de Transparencia), 124 y 125, de la abrogada Ley Federal de Transparencia y Acceso a la Información Pública (Ley Federal de Transparencia) [ambas leyes abrogadas el veinte de marzo de dos mil veinticinco] y 7 del Acuerdo General de Administración 5/2015, la estimó procedente y ordenó abrir el expediente UT/A/0106/2025.

TERCERO. Requerimiento de información. Mediante oficio UGTSIJ/TAIPDP-709-2025 del titular de la Unidad General de Transparencia, enviado por el Sistema de Gestión Documental Institucional el diecinueve de marzo de dos mil veinticinco, se requirió a la Dirección General de Tecnologías de la Información (Tecnologías de la Información) que se pronunciara sobre la información solicitada.

CUARTO. Informe de Tecnologías de la Información. El uno de abril de dos mil veinticinco, se remitió por el Sistema de Gestión Documental Institucional el oficio DGTI/168/2025, con el que, a su vez, se remitió la Atenta Nota con números *“DGTI-SGDS-11-2025 y DGTI-SGSICS-I-8-2025”*, de las Subdirecciones Generales de Desarrollo de Sistemas y de Seguridad Informática y Calidad de Sistemas, en la que se señala:

> *“En primera instancia, se aclara que, si bien el 20 de marzo de 2025 se publicó en el Diario Oficial de la Federación el DECRETO por el que se*

7O0pFAPhp5ZXGk3O3AgvT/mpeD17QD6U12ylATkfKBY=

expiden la Ley General de Transparencia y Acceso a la Información Pública; la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; la Ley Federal de Protección de Datos Personales en Posesión de los Particulares; y se reforma el artículo 37, fracción XV, de la Ley Orgánica de la Administración Pública Federal (del que se inserta vínculo electrónico para consulta), que abroga la normativa a la que se hace referencia en el presente oficio; el artículo Noveno Transitorio del referido Decreto indica que los procedimientos iniciados con anterioridad a su entrada en vigor, en materia de acceso a la información pública, se sustanciarán conforme a las disposiciones aplicables vigentes al momento de su inicio; en ese sentido, tomando en consideración que la solicitud que nos ocupa se recibió el 18 de marzo del presente año, es necesario emitir la respuesta con fundamento en las leyes de la materia vigentes al momento de su presentación.

Al respecto, se informa que la Dirección General de Tecnologías de la Información es competente para atender esta solicitud, de conformidad con lo previsto en el artículo 36 del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación, (del que se inserta liga electrónica), a través de las Subdirecciones Generales de Desarrollo de Sistemas y de Seguridad Informática y Calidad de Sistemas, cuyas funciones están relacionadas con la solicitud de mérito, por lo que se realizó una búsqueda exhaustiva y razonable de la información requerida en los archivos y registros con los que cuentan; en ese sentido, se proporciona la siguiente respuesta:

En primer lugar, se precisa que no existe obligación de la Dirección General de Tecnologías de la Información para generar un documento ad hoc, no obstante, lo anterior, en aras del principio de máxima publicidad se responde lo peticionado como sigue:

*Por lo que se refiere a la parte de la solicitud: 'Solicito se me proporcione información sobre el sistema, aplicación, herramienta o proceso electrónico de Inteligencia Artificial (IA) implementado por el Poder Judicial / Tribunal Superior de Justicia de * denominado "***', cualquier otro sistema de inteligencia artificial, cualquier otro sistema experto o cualquier sistema de automatización que permita: *Gestión de procesos *Gestión de documentos *Generación de documentos *Gestión de recursos informáticos *Gestión de recursos financieros *Análisis predictivo de casos *Generación de resúmenes de expedientes *Automatización de notificaciones *Cálculo de prestaciones *Cálculo de indemnizaciones *Ciberseguridad, se informa lo siguiente en cuanto a *Gestión de Documentos y *Ciberseguridad' se informa que, se cuenta con los sistemas de Gestión de Documentos denominados Buscador Jurídico y JusticIA 2.0.*

A. Aspectos Técnicos:
1. Nombre y versión de la herramienta, aplicación, sistema o proceso de IA. (sic)
Respuesta:
Nombre: Buscador Jurídico (BJ)
Versión de la herramienta: 2.0 Buscador Jurídico (del que se inserta vínculo electrónico para consulta).
Nombre: JusticIA

7O0pFAPhp5ZXGk3O3AgvT/mpeD17QD6U12ylATkfKBY=

Versión de la herramienta: 2.0 Transparencia Ciudadana (de la que se inserta vínculo electrónico para consulta).

2. Tipo de IA utilizada, por ejemplo, 'Aprendizaje automático, procesamiento del lenguaje natural, redes neuronales, sistemas expertos'). (sic)
Respuesta:
En ambos sistemas se hace uso del procesamiento de lenguaje natural.

3. Descripción de las funciones específicas que realiza la herramienta: (Ej. 'Análisis predictivo de casos, generación de resúmenes de expedientes, automatización de notificaciones, cálculo de indemnizaciones laborales'). (sic)
Respuesta:
La funcionalidad diseñada para ambos sistemas refiere a las búsquedas semánticas.

4. Algoritmos utilizados: (Ej. 'Regresión lineal, árboles de decisión, redes neuronales convolucionales'). (sic)
Respuesta:
En ambas se utilizan algoritmos de procesamiento de lenguaje natural.

5. Lenguajes de programación y tecnologías utilizadas en el desarrollo: (Ej. 'Python, Java, TensorFlow, PyTorch'). (sic)
Respuesta:
El lenguaje de programación en ambos sistemas es Java.

6. Arquitectura del sistema: (Ej. 'Sistema centralizado, sistema distribuido, basado en la nube'). (sic)
Respuesta:
La arquitectura de ambos sistemas se basa en servicios.

7. Datos de entrenamiento utilizados para la IA: (Ej. 'Base de datos de expedientes judiciales, legislación vigente'). (sic)
Respuesta:
No aplica, ya que no se realizan entrenamientos.

8. Proceso de validación y pruebas de la herramienta: (Ej. 'Metodología utilizada para asegurar la precisión y confiabilidad de la IA'). (sic)
Respuesta:
Son etapas del proceso de desarrollo y liberación de un sistema definido en la Suprema Corte de Justicia de la Nación.

9. Medidas de seguridad implementadas para proteger la información: (Ej. 'Cifrado de datos, controles de acceso'). (sic)
Respuesta:
Se cuenta con las herramientas de protección descritas en el servicio del Centro de Operaciones de Ciberseguridad.

10. Capacidad de auditoría del sistema: (Ej. 'Registros de actividad, trazabilidad de las decisiones'). (sic)
Respuesta:
No aplica, ya que ambos sistemas son buscadores, no toman decisiones.

7O0pFAPhp5ZXGk3O3AgvT/mpeD17QD6U12ylATkfKBY=

B. Aspectos Presupuestales:
Respuesta:
Se informa que los sistemas han sido desarrollados al interior de la Suprema Corte de Justicia de la Nación, por personal adscrito a la Subdirección General de Desarrollo de Sistemas de la Dirección General de Tecnologías de la Información, quienes atienden diversos proyectos, además de dar mantenimiento y soporte técnico a otros sistemas; luego entonces no se cuenta con un presupuesto específico asignado

C. Aspectos de Funcionamiento y Administración:
1. Criterios de selección e implementación de la herramienta: (Justificación de su uso). (sic)
Respuesta:
No aplica, ya que la Suprema Corte de Justicia de la Nación desarrolló los sistemas, por tal motivo no existe un proceso de selección.

2. Personal encargado de la operación y mantenimiento de la herramienta: (Número y perfil; sin nombres). (sic)
Respuesta:
2 subdirectores de área, 3 profesionales operativos y 1 técnico operativo.

3. Procedimientos de uso de la herramienta por parte de los funcionarios judiciales:
(Manuales o guías).
Respuesta:
Al respecto se proporcionan los enlaces del Buscador Jurídico y JusticIA en donde se pueden consultar el manual y el aparato de JusticIA.

4. Impacto de la herramienta en la eficiencia y tiempos de resolución de casos: (Estadísticas o estudios). (sic)
Respuesta:
No aplica, ya que los sistemas antes mencionados no resuelven casos.

5. Mecanismos de evaluación del desempeño de la herramienta: (Indicadores clave de rendimiento). (sic)
Respuesta:
La evaluación se lleva a cabo analizando el tiempo de respuesta de cada sistema y su capacidad de manejo de concurrencia, adaptándonos a la infraestructura con que actualmente cuenta la Suprema Corte de Justicia de la Nación.

6. Políticas de privacidad y protección de datos personales relacionadas con el uso de la IA: (Cumplimiento con la normatividad vigente). (sic)
Respuesta:
No aplica, ya que a través de esas herramientas no se da tratamiento a datos personales (Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos).

7O0pFAPhp5ZXGk3O3AgvT/mpeD17QD6U12ylATkfKBY=

7. Mecanismos de atención a quejas o errores en el funcionamiento de la IA: (Protocolos de actuación). (sic)
Respuesta:
No aplica, ya que la tecnología que se está utilizando, no toma decisiones y no hay procesos automáticos que afecten a la ciudadanía.

8. Transparencia en el uso de la IA en los procesos judiciales: (Información pública disponible para las partes). (sic)
Respuesta:
No aplica, ya que los sistemas desarrollados no participan ni forman parte de los procesos judiciales.

Adicional a lo anterior, se considera que la Ponencia de la Ministra Ana Margarita Ríos Farjat, podría pronunciarse en relación con la aplicación denominada Sor Juana.

En otro orden de ideas, en cuanto a Ciberseguridad se informa que:

Se cuenta con un Servicio Administrado de un Centro de Operaciones de Ciberseguridad (COC), mediante el cual se hace uso de herramientas con Inteligencia Artificial para la automatización de las acciones de contención de eventos para la protección de los activos informáticos de la Suprema Corte de Justicia de la Nación.

A. Aspectos Técnicos:
1. Nombre y versión de la herramienta, aplicación, sistema o proceso de IA. Se comunica que la información solicitada se considera reservada, de conformidad con los artículos 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP) y 113, fracción Vll de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), mediante la siguiente prueba de daño:

- *Existe un riesgo real, demostrable e identificable de perjuicio significativo al interés público, toda vez que la difusión de los nombres y versiones de las herramientas con Inteligencia Artificial para la automatización de las acciones de contención de eventos para la protección de los activos informáticos de la SCJN, gestionadas por un Servicio Administrado de un Centro de Operaciones de Ciberseguridad (COC), implicaría colocar en un estado de vulnerabilidad a la Suprema Corte de Justicia de la Nación, ya que al entregar dicha información se comprometería la seguridad informática de los sistemas y equipos de este Alto Tribunal, porque se pondría en riesgo la seguridad operativa de la infraestructura tecnológica que permite la operación de las diversas áreas del Alto Tribunal. En este sentido, la divulgación de la información permitiría:*

    - *Establecer con un alto grado de precisión la información técnica referente a los protocolos de seguridad y las características de la infraestructura instalada;*

    - *Dar a conocer puntos de vulnerabilidad sobre la infraestructura de seguridad informática encargada de proteger los sistemas, equipos informáticos y de cómputo de la institución;*

7O0pFAPhp5ZXGk3O3AgvT/mpeD17QD6U12ylATkfKBY=

- *Potenciar la posibilidad de vulnerar la seguridad de la infraestructura tecnológica institucional, permitiendo incluso el acceso ilícito a los sistemas y equipos informáticos de la institución, intentando la suplantación de estos;*

- *Poner en un estado vulnerable a la institución, facilitando la intervención de las comunicaciones y permitiendo usurpar permisos requeridos en la red para obtener información;*

- *Vulnerar sus sistemas informáticos, así como la información contenida en éstos;*

- *Atentar en contra de la infraestructura tecnológica, afectando el ejercicio de sus labores sustantivas, y*

- *Modificaría, destruiría o provocaría pérdida de información contenida en sus sistemas.*

- *Clasificar la información como reservada se adecua al principio de proporcionalidad, en tanto que se justifica negar su divulgación se motiva en pretender evitar o prevenir la comisión del delito de acceso ilícito a sus equipos y sistemas informáticos. Ello, aunado a que la clasificación constituye el medio menos lesivo para la adecuada protección del bien jurídico tutelado, como es la seguridad pública general.*

  Al respecto el Código Penal Federal dispone lo siguiente:

'TITULO NOVENO
Revelación de secretos y acceso ilícito a sistemas y equipos de informática
(…)
CAPÍTULO II
Acceso ilícito a sistemas y equipos de informática

ARTICULO 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.
Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

ARTICULO 211 BIS 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos
días de multa.
Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días de multa.
A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido

7O0pFAPhp5ZXGk3O3AgvT/mpeD17QD6U12ylATkfKBY=

> *servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.*
> *Las sanciones anteriores se duplicarán cuando la conducta obstruya, entorpezca, obstaculice, limite o imposibilite la procuración o impartición de justicia, o recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes.*
>
> *ARTICULO 211 bis 7.- Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.' (sic)*

De los preceptos antes citados, se advierte que comete el delito de acceso ilícito a sistemas y equipo de informática todo aquel que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, sean o no propiedad del Estado.

Asimismo, mencionan que, a quien sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días de multa.

De igual forma, la entrega de los nombres y versiones de las herramientas con Inteligencia Artificial para la automatización de las acciones de contención de eventos para la protección de los activos informáticos de la Suprema Corte de Justicia de la Nación podría ocasionar lo siguiente:

- *Una posible intervención de sus comunicaciones;*
- *La afectación de la disponibilidad de sus sistemas críticos, y*
- *El detrimento de su infraestructura tecnológica.*

Cuestiones que se materializan con la comisión de delitos de carácter cibernético, que sin duda afectarían severamente le ejercicio de las labores cotidianas y sustantivas de la Suprema Corte de Justicia de la Nación.

- *Con base en lo anterior, el riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda la información, ya que el resguardo de la información requerida en la solicitud implica llevar a cabo la prevención del delito de acceso ilícito a sistemas y equipos de informática tipificado en el Código Penal Federal, lo cual cobra importancia si se considera que dicha conducta implica conocer, copiar, modificar, destruir o provocar la pérdida de información contenida en sistemas o equipos de informática, por lo que revelar los nombres y versiones de las herramientas con Inteligencia Artificial para la automatización de las acciones de contención de eventos para la protección de los activos informáticos de la SCJN, gestionadas por un Servicio Administrado de un Centro de Operaciones de Ciberseguridad (COC), no sólo comprometería la información que obra en los archivos digitales del sujeto obligado, sino que menoscabaría la seguridad y certeza de las personas que acuden a este Alto Tribunal para otorgar certeza respecto de la impartición de justicia y control constitucional.*

7O0pFAPhp5ZXGk3O3AgvT/mpeD17QD6U12ylATkfKBY=

Por todo lo anterior, se advierte que difundir la información requerida incrementa sustancialmente la posibilidad de que aquella persona que conozca dicha información cometa algún ilícito, accediendo de forma no autorizada a los sistemas de datos que no son públicos en posesión del sujeto obligado, conociendo con un alto grado de precisión la información técnica y las características de su infraestructura de seguridad informática instalada, los protocolos de seguridad asociados o las vulnerabilidades de dicha infraestructura.

Ahora bien, en cuanto al periodo de reserva, el artículo 99 de la LFTAIP, establece que la información clasificada podrá permanecer con tal carácter, hasta por un periodo de cinco años, en el caso concreto, considerando que el bien jurídico tutelado es la prevención de un delito, se considera que el periodo de reserva debe ser de 5 años.

2. Tipo de IA utilizada, por ejemplo, 'Aprendizaje automático, procesamiento del lenguaje natural, redes neuronales, sistemas expertos').
Respuesta:
Aprendizaje automático.

3. Descripción de las funciones específicas que realiza la herramienta: (Ej. 'Análisis predictivo de casos, generación de resúmenes de expedientes, automatización de notificaciones, cálculo de indemnizaciones laborales'
Respuesta:
Contención de software malicioso.
Contención de correo malicioso.

4. Algoritmos utilizados: (Ej. 'Regresión lineal, árboles de decisión, redes neuronales convolucionales'). (sic)
5. Lenguajes de programación y tecnologías utilizadas en el desarrollo: (Ej. 'Python, Java, TensorFlow, PyTorch'). (sic)
7. Datos de entrenamiento utilizados para la IA: (Ej. 'Base de datos de expedientes judiciales, legislación vigente'). (sic)
Respuesta:
Al tratarse de soluciones que provee un prestador de servicios, no se cuenta con dicha información; por lo tanto, es inexistente con fundamento en el artículo 13 de la Ley Federal de Transparencia y Acceso a la Información Pública.

6. Arquitectura del sistema: (Ej. 'Sistema centralizado, sistema distribuido, basado en la nube').
Respuesta:
Sistemas basados en la nube.

8. Proceso de validación y pruebas de la herramienta: (Ej. 'Metodología utilizada para asegurar la precisión y confiabilidad de la IA').
Reportes mensuales relativos a los incidentes de seguridad informática y comportamientos anómalos detectados por el servicio y su solución (automática o por parte del COC).

9. Medidas de seguridad implementadas para proteger la información: (Ej. 'Cifrado de datos, controles de acceso').

7O0pFAPhp5ZXGk3O3AgvT/mpeD17QD6U12ylATkfKBY=

Respuesta:
Control de accesos y cifrado de datos.

10. Capacidad de auditoría del sistema: (Ej. 'Registros de actividad, trazabilidad de las decisiones').
Respuesta:
Cada sistema cuenta con registros de actividad.

B. Aspectos Presupuestales:
1. Costo de adquisición o desarrollo de la herramienta: (Desglosado si es posible).
2. Costo de mantenimiento y actualización: (Anual o periódico).
Respuesta:
Los costos relacionados se encuentran en el contrato SCJN/DGRM/DPC-038/12/2023, página 4 de 20 (del que se inserta vínculo electrónico para consulta).

3. Fuente de financiamiento: (Ej. 'Presupuesto del tribunal, fondos federales, donaciones').
Respuesta:
Presupuesto de la Suprema Corte de Justicia de la Nación.

4. Contratos con proveedores: (En caso de haberlos, solicitar una versión pública o resumida).
Respuesta:
El contrato que se encuentra vigente es SCJN/DGRM/DPC-038/12/2023 (del que se inserta vínculo electrónico para consulta).

C. Aspectos de Funcionamiento y Administración:
1. Criterios de selección e implementación de la herramienta: (Justificación de su uso).
Respuesta:
Metodología de investigación denominada 'Gartner Magic Quadrant'.

2. Personal encargado de la operación y mantenimiento de la herramienta: (Número y perfil; sin nombres).
El personal encargado de la operación y mantenimiento de las herramientas está a cargo del prestador de servicios del COC, página 38, 39 y 40 (se inserta vínculo electrónico para consulta) del Anexo 2ª Propuesta Técnica de la licitación pública nacional LPN/SCJN/DGRM/005/2023 para la contratación del servicio administrado del Centro de Operación de Ciberseguridad.

3. Procedimientos de uso de la herramienta por parte de los funcionarios judiciales: (Manuales o guías).
Respuesta:
No aplica, ya que son herramientas gestionadas por un prestador de servicios.

4. Impacto de la herramienta en la eficiencia y tiempos de resolución de casos: (Estadísticas o estudios). (sic)
Las herramientas bloquean de manera automática los intentos de ataque, software o correos maliciosos identificados.

7O0pFAPhp5ZXGk3O3AgvT/mpeD17QD6U12ylATkfKBY=

5. Mecanismos de evaluación del desempeño de la herramienta: (Indicadores clave de rendimiento). (sic)
Respuesta:
Se cuenta con reportes mensuales relativos a los incidentes de seguridad informática y comportamientos anómalos detectados por el servicio y su solución (automática o por parte del COC).

6. Políticas de privacidad y protección de datos personales relacionadas con el uso de la IA: (Cumplimiento con la normatividad vigente). (sic)
No aplica, ya que la información procesada corresponde a intentos de ataque a servicios o infraestructura tecnológica, software o correos maliciosos y no a datos personales.

7. Mecanismos de atención a quejas o errores en el funcionamiento de la IA: (Protocolos de actuación).
No aplica con relación al funcionamiento específico de la IA; sin embargo, el prestador de servicios adjudicado proporciona asistencia técnica, atención de incidentes/requerimientos/reportes en una modalidad 24x7x365 a través de los siguientes medios: asistencia vía telefónica para comunicación con el Centro de Operaciones en Ciberseguridad, asistencia vía correo electrónico, asistencia remota (software de conexión remota/ VPN site to site/ software de videoconferencia), asistencia vía mensajería instantánea (WhatsApp/Telegram), asistencia presencial en las oficinas de la SCJN en la CDMX (a demanda) y finalmente, una matriz de escalación multinivel, en la que se incluirá el nombre de contacto, número celular, rol y nivel de atención.

8. Transparencia en el uso de la IA en los procesos judiciales: (Información pública disponible para las partes). (sic)
No aplica, ya que la solución no forma parte de los procesos judiciales.

7O0pFAPhp5ZXGk3O3AgvT/mpeD17QD6U12yIATkfKBY=

QUINTO. Ampliación del plazo. Con el oficio UGTSIJ/TAIPDP-843-2025, enviado por correo electrónico el ocho de abril de dos mil veinticinco, la Unidad General de Transparencia solicitó la ampliación del plazo de respuesta, la cual fue autorizada por este Comité en sesión de nueve de abril último y así lo informó la Secretaria del Comité con el oficio CT-105-2025 y se notificó a la persona solicitante en la Plataforma Nacional de Transparencia y por correo electrónico el diez de abril de este año.

SEXTO. Ampliación de gestiones. Mediante oficio UGTSIJ/TAIPDP-846-2025, enviado por correo electrónico el diez de

abril de dos mil veinticinco, la Unidad General de Transparencia requirió a la Coordinación de la Ponencia de la Ministra Ana Margarita Ríos Farjat, para que en el ámbito de su competencia se pronunciara sobre la existencia, clasificación y disponibilidad de la información solicitada respecto de la aplicación denominada “Sor Juana”, haciéndole saber lo señalado por Tecnologías de la Información.

SÉPTIMO. Vista a la Secretaría del Comité de Transparencia. Mediante correo electrónico de once de abril de dos mil veinticinco, la Unidad General de Transparencia remitió el oficio UGTSIJ/TAIPDP-873-2025 y el expediente electrónico UT-A/0106/2025 a la Secretaría del Comité de Transparencia.

OCTAVO. Acuerdo de turno. En acuerdo de once de abril de dos mil veinticinco, con fundamento en los artículos 44, fracción II, de la Ley General de Transparencia, 23, fracción II, y 27, del Acuerdo General de Administración 5/2015, la Presidencia del Comité de Transparencia ordenó integrar el expediente **CT-VT/A-11-2025** y, conforme al turno correspondiente, remitirlo al Contralor del Alto Tribunal, lo que se hizo mediante oficio CT-109-2025, enviado por correo electrónico en la misma fecha.

C O N S I D E R A C I O N E S:

PRIMERA. Competencia. Para determinar el fundamento de la competencia de este Comité de Transparencia para conocer y resolver sobre el presente asunto, se recuerda que el veinte de marzo de dos mil veinticinco se publicó en el Diario Oficial de la Federación (DOF) el *DECRETO por el que se expiden la Ley General de Transparencia y Acceso a la Información Pública; la Ley General de Protección de Datos*

7O0pFAPhp5ZXGk3O3AgvT/mpeD17QD6U12ylATkfKBY=

Personales en Posesión de Sujetos Obligados; la Ley Federal de Protección de Datos Personales en Posesión de los Particulares; y se reforma el artículo 37, fracción XV, de la Ley Orgánica de la Administración Pública Federal, cuyo artículo Segundo Transitorio estableció la **abrogación** de diversas leyes, entre ellas, la Ley General de Transparencia publicada en el DOF el cuatro de mayo de dos mil quince y la Ley Federal de Transparencia publicada en el DOF el nueve de mayo de dos mil dieciséis.

Ante esta circunstancia, resulta conveniente señalar que los artículos Noveno y Décimo Transitorios del propio decreto establecen que los **procedimientos iniciados** ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) **con anterioridad a su entrada en vigor**, en materias de acceso a la información pública, y de datos personales o cualquier otra distinta a la mencionada en el transitorio Noveno, se sustanciarían ante Transparencia para el Pueblo o ante la Secretaría Anticorrupción y Buen Gobierno, respectivamente, conforme a las **disposiciones aplicables vigentes al momento de su inicio**.

Ahora, se destaca que el procedimiento de acceso a la información pública se compone por diversas etapas, las cuales, genéricamente, inician con la presentación de la solicitud, continúan con los trámites a cargo de la Unidad de Transparencia, con la posibilidad de participación del Comité de Transparencia para confirmar, modificar o revocar las determinaciones sobre clasificación, declaración de inexistencia o incompetencia, así como ampliación del plazo tratándose de información reservada que realicen las instancias competentes y, en su caso, con la impugnación ante el INAI de la respuesta otorgada por el sujeto obligado del orden federal.

7O0pFAPhp5ZXGk3O3AgvT/mpeD17QD6U12ylATkfKBY=

En ese sentido, tomando en cuenta que la previsión en los transitorios fue únicamente para los medios de impugnación ante el INAI y que, con base en el principio de analogía jurídica, se puede aplicar una solución prevista en la ley a un caso no regulado, pero similar a aquel, puede concluirse válidamente que la legislación abrogada a través del decreto de veinte de marzo del presente año, resulta aplicable a las solicitudes de acceso a la información que se encuentren en trámite ante este Alto Tribunal que se hubieran presentado con anterioridad a la entrada en vigor del decreto en comento, esto es, antes del veintiuno de marzo de dos mil veinticinco.

En el caso concreto, se advierte que la solicitud de acceso a la información se presentó en la Plataforma Nacional de Transparencia el dieciocho de marzo de dos mil veinticinco, fecha en la que aún estaban vigentes la Ley General de Transparencia publicada en el DOF el cuatro de mayo de dos mil quince y la Ley Federal de Transparencia publicada en el DOF el nueve de mayo de dos mil dieciséis, por tanto, se concluye que para el resto de las etapas de ese procedimiento que correspondan a este Alto Tribunal, resultan aplicables dichas Leyes.

A partir de lo expuesto, el Comité de Transparencia de la Suprema Corte de Justicia de la Nación es competente para conocer y resolver el presente asunto, en términos de los artículos 6° de la Constitución Política de los Estados Unidos Mexicanos, 4 y 44, fracciones I y II, de la Ley General de Transparencia publicada en el DOF el cuatro de mayo de dos mil quince, 65, fracciones I y II, de la Ley Federal de Transparencia publicada en el DOF el nueve de mayo de dos mil dieciséis; así como 23, fracciones I y II, del Acuerdo General de Administración 5/2015.

7O0pFAPhp5ZXGk3O3AgvT/mpeD17QD6U12ylATkfKBY=

SEGUNDA. Análisis. En solicitud se pide información sobre un sistema de aplicación, herramienta o proceso electrónico de Inteligencia Artificial implementado por el *“Poder Judicial / Tribunal Superior de Justicia”* que permita:

- Gestión de procesos.
- Gestión de documentos.
- Generación de documentos.
- Gestión de recursos informáticos.
- Gestión de recursos financieros.
- Análisis predictivo de casos.
- Generación de resúmenes de expedientes.
- Automatización de notificaciones
- Cálculo de prestaciones.
- Cálculo de indemnizaciones.
- Ciberseguridad.

A partir de los rubros: A. Aspectos Técnicos, B. Aspectos Presupuestales y C. Aspectos de Funcionamiento y Administración.

Al respecto, Tecnologías de la Información -a través de la nota de las Subdirecciones Generales de Desarrollo de Sistemas y de Seguridad Informática y Calidad de Sistemas- refiere que no está obligada a generar un documento *ad hoc*, pero en observancia al principio de máxima publicidad, atiende la solicitud señalando que la Suprema Corte de Justicia de la Nación utiliza los sistemas denominados *Buscador Jurídico* y *JusticIA 2.0*, para funciones relacionadas con la *Gestión de Documentos* y, sobre el rubro de *Ciberseguridad*, refiere que se cuenta con un Servicio Administrado de

7O0pFAPhp5ZXGk3O3AgvT/mpeD17QD6U12ylATkfKBY=

un Centro de Operaciones de Ciberseguridad, mediante el cual se hace uso de herramientas con inteligencia artificial para la automatización de las acciones de contención de eventos para la protección de los activos informáticos de este Alto Tribunal.

En ese sentido, para facilitar la comprensión de la respuesta otorgada a cada uno de los puntos que plantea la solicitud, en la siguiente tabla se presenta la información solicitada y la respuesta que Tecnologías de la Información emitió sobre cada planteamiento:

Información solicitada	**Respuesta**	
	Gestión de documentos	***Ciberseguridad***
A. Aspectos técnicos		
1. Nombre y versión de la herramienta, aplicación, sistema o proceso de IA.	Nombre: *Buscador Jurídico* Versión de la herramienta: 2.0 *Buscador Jurídico* Nombre: *JusticIA* Versión de la herramienta: 2.0 Transparencia Ciudadana	La información es reservada, con apoyo en los artículos 110, fracción VII, de la Ley Federal de Transparencia y 113, fracción VII, de la Ley General de Transparencia.
2. Tipo de IA utilizada, por ejemplo, "Aprendizaje automático, procesamiento del lenguaje natural, redes neuronales, sistemas expertos").	En ambos sistemas se hace uso del procesamiento de lenguaje natural.	Aprendizaje automático.
3. Descripción de las funciones específicas que realiza la herramienta: (Ej. "Análisis predictivo de casos, generación de resúmenes de expedientes, automatización de notificaciones, cálculo de indemnizaciones laborales").	La funcionalidad diseñada para ambos sistemas refiere a las búsquedas semánticas.	Contención de *software* malicioso. Contención de correo malicioso.
4. Algoritmos utilizados: (Ej. "Regresión lineal, árboles de decisión, redes neuronales convolucionales").	En ambas se utilizan algoritmos de procesamiento de lenguaje natural.	No aplica porque se trata de soluciones que provee un prestador de servicios.
5. Lenguajes de programación y tecnologías utilizadas en el desarrollo: (Ej. "Python, Java, TensorFlow, PyTorch").	El lenguaje de programación en ambos sistemas es *Java*.	No aplica porque se trata de soluciones que provee un prestador de servicios.
6. Arquitectura del sistema: (Ej. "Sistema centralizado, sistema distribuido, basado en la nube").	La arquitectura de ambos sistemas se basa en servicios.	Sistemas basados en la nube.

7O0pFAPhp5ZXGk3O3AgvT/mpeD17QD6U12ylATkfKBY=

Información solicitada	Respuesta	
	Gestión de documentos	***Ciberseguridad***
7. Datos de entrenamiento utilizados para la IA: (Ej. "Base de datos de expedientes judiciales, legislación vigente").	No aplica, ya que no se realizan entrenamientos.	No aplica porque se trata de soluciones que provee un prestador de servicios.
8. Proceso de validación y pruebas de la herramienta: (Ej. "Metodología utilizada para asegurar la precisión y confiabilidad de la IA").	Son etapas del proceso de desarrollo y liberación de un sistema definido en la Suprema Corte de Justicia de la Nación (SCJN).	Reportes mensuales relativos a los incidentes de seguridad informática y comportamientos anómalos detectados por el servicio y su solución (automática o por parte del Centro de Operaciones de Ciberseguridad).
9. Medidas de seguridad implementadas para proteger la información: (Ej. "Cifrado de datos, controles de acceso").	Se cuenta con las herramientas de protección descritas en el servicio del Centro de Operaciones de Ciberseguridad.	Control de accesos y cifrado de datos.
10. Capacidad de auditoría del sistema: (Ej. "Registros de actividad, trazabilidad de las decisiones").	No aplica, ya que ambos sistemas son buscadores, no toman decisiones.	Cada sistema cuenta con registros de actividad.
B. Aspectos Presupuestales:		
1. Costo de adquisición o desarrollo de la herramienta: (Desglosado si es posible).	Los sistemas han sido desarrollados al interior de la SCJN, por personal adscrito a la Subdirección General de Desarrollo de Sistemas, quienes atienden diversos proyectos, además de dar mantenimiento y soporte técnico a otros sistemas, por ese motivo no se cuenta con un presupuesto específico asignado	Los costos relacionados se encuentran en el contrato SCJN/DGRM/DPC-038/12/2023, página 4 de 20.
2. Costo de mantenimiento y actualización: (Anual o periódico).		
3. Fuente de financiamiento: (Ej. "Presupuesto del tribunal, fondos federales, donaciones").		Presupuesto de la SCJN.
4. Contratos con proveedores: (En caso de haberlos, solicitar una versión pública o resumida).		El contrato que se encuentra vigente es SCJN/DGRM/DPC-038/12/2023.
C. Aspectos de Funcionamiento y Administración:		
1. Criterios de selección e implementación de la herramienta: (Justificación de su uso).	No aplica, ya que la SCJN desarrolló los sistemas, por tal motivo no existe un proceso de selección.	Metodología de investigación denominada *"Gartner Magic Quadrant".*
2. Personal encargado de la operación y mantenimiento de la herramienta: (Número y perfil; sin nombres).	Dos subdirectores de área, tres profesionales operativos y un técnico operativo	El personal encargado de la operación y mantenimiento de las herramientas está a cargo del prestador de servicios del Centro de Operaciones de Ciberseguridad, página 38, 39 y 40, del Anexo 2ª Propuesta Técnica de la licitación pública nacional LPN/SCJN/DGRM/005/2023 para la contratación del servicio administrado del Centro de Operación de Ciberseguridad.

7O0pFAPhp5ZXGk3O3AgvT/mpeD17QD6U12ylATkfKBY=

Información solicitada	Respuesta	
	Gestión de documentos	***Ciberseguridad***
3. Procedimientos de uso de la herramienta por parte de los funcionarios judiciales: (Manuales o guías).	Se proporcionan los enlaces del *Buscador Jurídico* y *JusticIA* en donde se pueden consultar el manual y el aparato de *JusticIA*.	No aplica, ya que son herramientas gestionadas por un prestador de servicios.
4. Impacto de la herramienta en la eficiencia y tiempos de resolución de casos: (Estadísticas o estudios).	No aplica, ya que los sistemas antes mencionados no resuelven casos.	Las herramientas bloquean de manera automática los intentos de ataque, software o correos maliciosos identificados.
5. Mecanismos de evaluación del desempeño de la herramienta: (Indicadores clave de rendimiento).	La evaluación se lleva a cabo analizando el tiempo de respuesta de cada sistema y su capacidad de manejo de concurrencia, adaptándonos a la infraestructura con que actualmente cuenta la SCJN.	Se cuenta con reportes mensuales relativos a los incidentes de seguridad informática y comportamientos anómalos detectados por el servicio y su solución (automática o por parte del Centro de Operaciones de Ciberseguridad).
6. Políticas de privacidad y protección de datos personales relacionadas con el uso de la IA: (Cumplimiento con la normatividad vigente).	No aplica, ya que a través de esas herramientas no se da tratamiento a datos personales (cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos).	No aplica, ya que la información procesada corresponde a intentos de ataque a servicios o infraestructura tecnológica, *software* o correos maliciosos y no a datos personales.

7O0pFAPhp5ZXGk3O3AgvT/mpeD17QD6U12ylATkfKBY=

Información solicitada	Respuesta	
	Gestión de documentos	***Ciberseguridad***
7. Mecanismos de atención a quejas o errores en el funcionamiento de la IA: (Protocolos de actuación).	No aplica, ya que la tecnología que se está utilizando, no toma decisiones y no hay procesos automáticos que afecten a la ciudadanía.	No aplica con relación al funcionamiento específico de la inteligencia artificial; sin embargo, el prestador de servicios adjudicado proporciona asistencia técnica, atención de incidentes/requerimientos/reportes en una modalidad 24x7x365 a través de los siguientes medios: asistencia vía telefónica para comunicación con el Centro de Operaciones en Ciberseguridad, asistencia vía correo electrónico, asistencia remota (*software* de conexión remota/ VPN *site to site/ software* de videoconferencia), asistencia vía mensajería instantánea (*WhatsApp/Telegram*), asistencia presencial en las oficinas de este Alto Tribunal en la Ciudad de México (a demanda) y finalmente, una matriz de escalación multinivel, en la que se incluirá el nombre de contacto, número celular, rol y nivel de atención.
8. Transparencia en el uso de la IA en los procesos judiciales: (Información pública disponible para las partes).	No aplica, ya que los sistemas desarrollados no participan ni forman parte de los procesos judiciales.	No aplica, ya que la solución no forma parte de los procesos judiciales.

Para realizar el análisis de lo anterior, se tiene en cuenta, en primer término, que de conformidad con el artículo 100, último párrafo, de la Ley General de Transparencia[1], en relación con el artículo 17, párrafo primero, del Acuerdo General de Administración 5/2015[2], es competencia de la instancia que tiene bajo resguardo la información determinar su disponibilidad y clasificarla conforme a los criterios establecidos en la normativa aplicable, por lo que debe destacarse que el pronunciamiento que se analizará está hecho por el área técnica de

[1] *"**Artículo 100.** (…)*
Los titulares de las Áreas de los sujetos obligados serán los responsables de clasificar la información, de conformidad con lo dispuesto en esta Ley, la Ley Federal y de las Entidades Federativas."
[2] *"**Artículo 17 De la responsabilidad de los titulares y los enlaces***
En su ámbito de atribuciones, los titulares de las instancias serán responsables de la gestión de las solicitudes, así como de la veracidad y confiabilidad de la información…"

7O0pFAPhp5ZXGk3O3AgvT/mpeD17QD6U12ylATkfKBY=

este Alto Tribunal, a la que corresponde, en su caso, el resguardo de la información solicitada.

1. Aspectos atendidos.

1.1. Aspectos técnicos.

Se tiene por atendido lo solicitado en el punto 1, sobre el nombre y versión de las herramientas de inteligencia artificial, ya que se proporciona dicha información para el *Buscador Jurídico* y *JusticIA*, incluyendo los hipervínculos correspondientes para su consulta.

Por cuanto hace al nombre y versión de la herramienta de *Ciberseguridad*, el análisis de la clasificación que se plantea se realizará en otro apartado.

También se atiende el punto 2, relativo al tipo de inteligencia artificial utilizada, pues se señala que el *Buscador Jurídico* y *JusticIA* emplean lenguaje natural y que la herramienta de Ciberseguridad utiliza aprendizaje automático.

Se tiene también por atendida la descripción de las funciones específicas de las herramientas a que hace referencia el punto 3, al indicarse que el *Buscador Jurídico* y *JusticIA* realizan búsqueda semántica, mientras que la herramienta de Ciberseguridad se orienta a la contención de *software* y correos maliciosos.

Igualmente, se tiene por atendido lo relativo a los algoritmos utilizados, que corresponde al punto 4, pues se precisa que en el *Buscador Jurídico* y *JusticIA* se emplean algoritmos de procesamiento de lenguaje natural y en la herramienta de Ciberseguridad, soluciones del proveedor.

7O0pFAPhp5ZXGk3O3AgvT/mpeD17QD6U12ylATkfKBY=

En relación con el lenguaje de programación y tecnologías utilizadas a que hace referencia el punto 5, se tiene por atendido al señalarse que el *Buscador Jurídico* y *JusticIA* se desarrollaron en *Java*, y que la solución de Ciberseguridad es proporcionada por el proveedor.

Se atiende el punto 6 sobre la arquitectura del sistema, al señalarse que el *Buscador Jurídico* y *JusticIA* se basan en arquitectura de servicios, mientras que la Ciberseguridad en sistemas en la nube.

También se tiene por atendido lo referente a los datos de entrenamiento, punto 7, pues se aclara que ni el *Buscador Jurídico* ni *JusticIA* requieren entrenamiento, y que la herramienta de Ciberseguridad opera con soluciones del proveedor.

En relación con el punto 8, concerniente al proceso de validación y pruebas, se considera atendido al haberse informado que el *Buscador Jurídico* y *JusticIA* siguen un proceso de desarrollo y liberación de un sistema definido por este Alto Tribunal, y que la herramienta de Ciberseguridad cuenta con reportes mensuales de incidentes.

Se considera atendido el punto 9, relativo a las medidas de seguridad, pues se informa que se emplean herramientas del Centro de Operaciones de Ciberseguridad, así como Control de Accesos y Cifrado de Datos.

Respecto del punto 10, relativo a la capacidad de auditoría, se señala que ello no aplica para el *Buscador Jurídico* ni para *JusticIA* porque su naturaleza es informativa, y que la herramienta de

7O0pFAPhp5ZXGk3O3AgvT/mpeD17QD6U12ylATkfKBY=

Ciberseguridad sí cuenta con registros de actividad, por lo que con esa información se atiende ese aspecto de la solicitud.

1.2. Aspectos Presupuestales.

Se atienden los puntos 1, 2, 3 y 4, sobre los temas de costo de desarrollo, mantenimiento, fuente de financiamiento y contratos, pues se informa que el *Buscador Jurídico* y *JusticIA* fueron desarrollados internamente, sin recursos presupuestales específicos, además, para la herramienta de Ciberseguridad se proporciona el hipervínculo del contrato SCJN/DGRM/DPC-038/12/2023, y se agrega que el financiamiento proviene del presupuesto del Alto Tribunal.

No pasa inadvertido que la persona solicitante pidió la información en modalidad de copia simple; sin embargo, atendiendo a lo establecido en el artículo 130[3] de la Ley General de Transparencia, el derecho de acceso a la información se garantiza cuando se indica la fuente, el lugar y la forma en que puede consultarse, de ahí que al indicarse el enlace electrónico en el que se puede consultar el instrumento contractual referido, se puede tener por atendido lo solicitado sobre ese aspecto.

1.3. Aspectos de funcionamiento y administración.

Se atiende el punto 1, sobre los criterios de selección e implementación, al indicarse que no aplica para el *Buscador Jurídico* ni para *JusticIA*, porque se desarrollaron internamente y, respecto de la herramienta de Ciberseguridad se menciona el uso de la metodología *“Gartner Magic Quadrant”.*

[3] *“**Artículo 130.** Cuando la información requerida por el solicitante ya esté disponible al público en medios impresos, tales como libros, compendios, trípticos, registros públicos, en formatos electrónicos disponibles en Internet o en cualquier otro medio, se le hará saber por el medio requerido por el solicitante la fuente, el lugar y la forma en que puede consultar, reproducir o adquirir dicha información en un plazo no mayor a cinco días.”*

7O0pFAPhp5ZXGk3O3AgvT/mpeD17QD6U12ylATkfKBY=

También se atiende el punto 2, relativo al número del personal encargado del *Buscador Jurídico* y *JusticIA*, pues se informa que se cuenta con dos subdirectores de área, tres profesionales operativos y un técnico operativo; además, por lo que hace a la operación de la herramienta de Ciberseguridad, se informa que el personal encargado de su operación y mantenimiento está a cargo del prestador de servicios, respecto de lo cual se proporciona el hipervínculo de la Propuesta Técnica de la licitación pública nacional LPN/SCJN/DGRM/005/2023 en la que se puede consultar el número de personas encargadas de esa herramienta y su perfil.

Cabe señalar que Tecnologías de la Información no se pronunció sobre el perfil del personal de la Suprema Corte de Justicia de la Nación; sin embargo, este Comité advierte que esa información es de carácter público y se encuentra disponible en el Catálogo General de Puestos[4], en el que, con la denominación del puesto, la persona solicitante puede consultar el perfil de cada uno de los cargos que refirió la instancia vinculada.

Por cuanto hace al punto 3 sobre manuales y guías de uso, se proporcionan los enlaces electrónicos para el *Buscador Jurídico* y para *JusticIA*, y se precisa que no aplica para la herramienta de Ciberseguridad, por ser gestionada por un prestador de servicios, de ahí que con esa información se atiende ese aspecto de la solicitud.

Se tiene por atendido el punto 4, referente al impacto en la eficiencia y tiempos de resolución, toda vez que se informa que no

7O0pFAPhp5ZXGk3O3AgvT/mpeD17QD6U12ylATkfKBY=

[4] Consultable en https://www.scjn.gob.mx/conoce-la-corte/marconormativo/public/api/download?fileName=CATALOGO%20GENERAL%20DE%20PUESTOS%20VERSION%20FINAL%20PUBLICABLE%20AUTORIZADO%2030-SEP-2019.pdf

aplica al *Buscador Jurídico* ni a *JusticIA* por no resolver casos, y que la herramienta de Ciberseguridad bloquea automáticamente ataques detectados.

De igual forma, se atiende lo relativo al punto 5 sobre mecanismos de evaluación del desempeño, al señalarse que el *Buscador Jurídico* y *JusticIA* se evalúan por tiempos de respuesta y capacidad de manejo de concurrencia, y que la herramienta de Ciberseguridad cuenta con reportes mensuales de incidentes.

Sobre el tema de políticas de privacidad y protección de datos personales referidos en el punto 6, se tiene por atendido porque se aclara que las referidas herramientas no tratan datos personales.

En cuanto a los mecanismos de atención de quejas o errores que corresponde al punto 7, se informa que no aplica para el *Buscador Jurídico* ni para *JusticIA*, y que la herramienta de Ciberseguridad cuenta con soporte técnico 24/7 por parte del prestador de servicios, de ahí que con esa información se atiende ese numeral de la solicitud.

También se atiende el punto 8, relativo a la transparencia en el uso de inteligencia artificial en procesos judiciales, debido a que se informa que no aplica para ninguna de las herramientas, al no formar parte de esos procesos.

De conformidad con lo expuesto, se encomienda a la Unidad General de Transparencia que haga del conocimiento de la persona solicitante la respuesta que se emitió sobre los aspectos de la solicitud que se tienen por atendidos en este apartado.

7O0pFAPhp5ZXGk3O3AgvT/mpeD17QD6U12ylATkfKBY=

2. Información reservada.

En relación con la herramienta de Ciberseguridad, Tecnologías de la Información clasificó como información reservada el nombre y versión de las herramientas con inteligencia artificial para la automatización de las acciones de contención de eventos para la protección de los activos informáticos de la Suprema Corte de Justicia de la Nación, gestionadas por un Servicio Administrado de un Centro de Operaciones de Ciberseguridad (punto 1), con apoyo en los artículos 110, fracción VII, de la Ley Federal de Transparencia y 113, fracción VII, de la Ley General de Transparencia (vigentes cuando se presentó la solicitud), pues se señala que revelar esa información podría poner en riesgo el acceso a los servicios de telecomunicaciones, tales como los sitios, esquemas de conectividad y de seguridad, así como equipos y tecnologías que se usan para salvaguardar la información y comunicaciones de este Alto Tribunal.

Para emitir pronunciamiento sobre la reserva de la información que se propone, se tiene en cuenta que el derecho de acceso a la información encuentra cimiento en lo dispuesto en el artículo 6º, apartado A, de la Constitución Política de los Estados Unidos Mexicanos, cuyo contenido deja claro que, en principio, todo acto de autoridad (todo acto de gobierno) es de interés general y, por ende, es susceptible de ser conocido por todas las personas.

Al respecto, el Pleno del Alto Tribunal ha interpretado, en diversas ocasiones, que el derecho de acceso a la información no puede caracterizarse como de contenido absoluto, en tanto su ejercicio se

7O0pFAPhp5ZXGk3O3AgvT/mpeD17QD6U12ylATkfKBY=

encuentra acotado en función de ciertas causas e intereses relevantes, así como frente al necesario tránsito de las vías adecuadas para ello[5].

En atención a la disposición constitucional referida, la información que tienen bajo su resguardo los sujetos obligados del Estado encuentra como excepción aquella que sea temporalmente reservada o confidencial en los términos establecidos por el legislador federal o local, cuando de su propagación pueda derivarse perjuicio por causa de interés público y seguridad nacional.

Ahora bien, para sustentar la reserva de la información referida en este apartado, la instancia vinculada señala que la divulgación de esa información:

- Establecería con un alto grado de precisión la información técnica referente a los protocolos de seguridad y las características de la infraestructura instalada.
- Daría a conocer puntos de vulnerabilidad sobre la infraestructura de seguridad informática encargada de proteger los sistemas, equipos informáticos y de cómputo de la institución.

7O0pFAPhp5ZXGk3O3AgvT/mpeD17QD6U12ylATkfKBY=

---

[5] ***DERECHO A LA INFORMACIÓN. SU EJERCICIO SE ENCUENTRA LIMITADO TANTO POR LOS INTERESES NACIONALES Y DE LA SOCIEDAD, COMO POR LOS DERECHOS DE TERCEROS****. El derecho a la información consagrado en la última parte del artículo 6o. de la Constitución Federal no es absoluto, sino que, como toda garantía, se halla sujeto a limitaciones o excepciones que se sustentan, fundamentalmente, en la protección de la seguridad nacional y en el respeto tanto a los intereses de la sociedad como a los derechos de los gobernados, limitaciones que, incluso, han dado origen a la figura jurídica del secreto de información que se conoce en la doctrina como "reserva de información" o "secreto burocrático". En estas condiciones, al encontrarse obligado el Estado, como sujeto pasivo de la citada garantía, a velar por dichos intereses, con apego a las normas constitucionales y legales, el mencionado derecho no puede ser garantizado indiscriminadamente, sino que el respeto a su ejercicio encuentra excepciones que lo regulan y a su vez lo garantizan, en atención a la materia a que se refiera; así, en cuanto a la seguridad nacional, se tienen normas que, por un lado, restringen el acceso a la información en esta materia, en razón de que su conocimiento público puede generar daños a los intereses nacionales y, por el otro, sancionan la inobservancia de esa reserva; por lo que hace al interés social, se cuenta con normas que tienden a proteger la averiguación de los delitos, la salud y la moral públicas, mientras que por lo que respecta a la protección de la persona existen normas que protegen el derecho a la vida o a la privacidad de los gobernados. Época: Novena Época. Registro: 191967. Instancia: Pleno. Tipo de Tesis: Aislada. Fuente: Semanario Judicial de la Federación y su Gaceta. Tomo XI, Abril de 2000. Materia(s): Constitucional Tesis: P. LX/2000. Página: 74)*

- Potenciaría la posibilidad de vulnerar la seguridad de la infraestructura tecnológica institucional, permitiendo, incluso, el acceso ilícito a los sistemas y equipos informáticos de la institución, intentando la suplantación de estos.
- Pondría en un estado vulnerable a la institución, facilitando la intervención de las comunicaciones y permitiendo usurpar permisos requeridos en la red para obtener información;
- Vulneraría sus sistemas informáticos, así como la información contenida en éstos.
- Atentaría contra la infraestructura tecnológica de este Alto Tribunal, afectando el ejercicio de sus labores sustantivas.
- Modificaría, destruiría o provocaría pérdida de información contenida en sus sistemas.

Como se señaló, la reserva de la información se fundamenta en los artículos 110, fracción VII, de la Ley Federal de Transparencia y 113, fracción VII, de la Ley General de Transparencia, entonces vigentes, bajo el argumento de que su divulgación revelaría detalles técnicos sobre la seguridad e infraestructura tecnológica de este Alto Tribunal, poniendo en riesgo la integridad de los sistemas y la información contenida en ellos, y se obstruiría la prevención de delitos, específicamente, el de acceso ilícito a sus equipos y sistemas de informática.

Al respecto, es importante destacar que el informe lo emite el área técnica que, conforme a las atribuciones que le confiere el artículo 36 del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación, es responsable de los servicios y sistemas informáticos sobre los que versa la solicitud que da origen a

7O0pFAPhp5ZXGk3O3AgvT/mpeD17QD6U12ylATkfKBY=

este asunto y, tomando como base lo resuelto por este Comité en el cumplimiento CT-CUM-R/A-2-2019[6], retomado en las resoluciones CT-VT/A-39-2022[7] y CT-VT/A-8-2025[8], en las que se analizó información similar, se arriba a la conclusión de que sobre los datos materia del presente apartado sí resulta aplicable la reserva establecida en la fracción VII del artículo 110, de la Ley Federal de Transparencia, el cual establece:

> ***"Artículo 110.*** *Conforme a lo dispuesto por el artículo 113 de la Ley General, como información reservada podrá clasificarse aquella cuya publicación:*
> (…)
> *VII. Obstruya la prevención o persecución de los delitos;"*
> (…)

Sobre el alcance del artículo 110, fracción VII, de la Ley Federal de Transparencia, se tiene en cuenta que su contenido es idéntico al del artículo 113, fracción VII[9], de la Ley General de Transparencia, por lo que es posible considerar lo resuelto por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) en el recurso de revisión RRA 10276/18, cumplimentado por este Comité en la resolución CT-CUM-R/A-2-2019, ya que se argumentó que *"como información reservada podrá clasificarse aquella cuya publicación obstruya la prevención o persecución de delitos",* a lo que se agregó que *"para que pueda acreditarse que la información requerida pudiera 'obstruir la prevención de los delitos', debe vincularse a la* ***afectación a las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de las autoridades para evitar la***

[6] Disponible en https://www.scjn.gob.mx/sites/default/files/resoluciones/2019-03/CT-CUM-R-A-2-2019.pdf
[7] Consultable en https://www.scjn.gob.mx/sites/default/files/resoluciones/2022-12/CT-VT-A-39-2022.pdf
[8] Consultable en https://www.scjn.gob.mx/sites/default/files/resoluciones/2025-04/CT-VT-A-8-2025.pdf
[9] *"**Artículo 113.** Como información reservada podrá clasificarse aquella cuya publicación:*
(…)
VII. Obstruya la prevención o persecución de los delitos;"
(…)

7O0pFAPhp5ZXGk3O3AgvT/mpeD17QD6U12ylATkfKBY=

comisión de delitos” (página 98 vuelta de la resolución del recurso de revisión RRA 10276/18).

Además, en dichas resoluciones se menciona que de esa causal de reserva se desprenden dos vertientes; una que se refiere a la prevención de los delitos y la otra a la persecución de los mismos y que *“por definición de la palabra **prevención** se hace referencia a medidas y acciones dispuestas con anticipación con el fin de evitar o impedir que se presente un fenómeno peligroso para reducir sus efectos sobre la publicación”,* de ahí que prevención del delito significa *“tomar medidas y realizar acciones para evitar una conducta o un comportamiento que puedan dañar o convertir a la población en sujetos o víctimas de un ilícito”*, por lo que desde el punto de vista criminológico prevenir es *“conocer con anticipación la probabilidad de una conducta criminal disponiendo de los medios necesarios para evitarla; es decir, no permitir que alguna situación llegue a darse porque ésta se estima inconveniente”.*

También se señaló en esas resoluciones que conforme al Código Penal Federal *“comete el **delito de acceso ilícito a sistemas y equipos de informática** todo aquel que **sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad**, sean o no propiedad del Estado. Asimismo, al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del **Estado**, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa”* (foja 100 vuelta de la resolución del recurso de revisión RRA 10276/18).

7O0pFAPhp5ZXGk3O3AgvT/mpeD17QD6U12ylATkfKBY=

Conforme a lo anterior, en la resolución del INAI se argumenta que *"derivado de la naturaleza y el grado de especificidad del tipo de información que se requiere, y que se trata de un elemento relevante al ponderar* ***cualquier posible vulneración a la seguridad de la infraestructura tecnológica*** *de la autoridad obligada, es que se colige que dar a conocer la misma facilitaría que personas expertas en informática* ***perturben el sistema de la infraestructura tecnológica*** *de la Suprema Corte de Justicia de la Nación, ejecuten programas informáticos perjudiciales que modifiquen o destruyan información relevante; situación que pondría en un estado vulnerable la información que en ella se contiene, facilitando la intervención de las comunicaciones y permitiendo usurpar permisos requeridos en la red para obtener información"*.

Atendiendo a los argumentos señalados en la resolución de cumplimiento CT-CUM-R/A-2-2019 y lo sostenido por el INAI en el recurso de revisión RRA 10276/18, se **confirma la reserva** del nombre y versión de la herramienta, aplicación, sistema o proceso de inteligencia artificial en cuanto a Ciberseguridad, con fundamento en los artículos 113, fracción VII, de la Ley General de Transparencia y 110, fracción VII, de la Ley Federal de transparencia, dado que, como se mencionó, Tecnologías de la Información es el área técnica con atribuciones para suscribir contratos sobre los servicios informáticos de los que se pide información y ha expuesto los argumentos que sostienen la naturaleza de esos datos, señalando que, al publicitarlos, se podría comprometer la seguridad informática de los sistemas y equipos de este Alto Tribunal, poniendo en riesgo la seguridad operativa de la infraestructura tecnológica que permite la operación de esos sistemas.

Análisis específico de la prueba de daño.

7O0pFAPhp5ZXGk3O3AgvT/mpeD17QD6U12ylATkfKBY=

Al hacer el análisis específico de la prueba de daño que prevén los artículos 103 y 104, de la Ley General de Transparencia, se tienen presentes los motivos que expuso la Dirección General de Tecnologías de la Información, así como lo argumentado en la resolución del INAI en el recurso de revisión RRA 10276/18 y por este Comité en la resolución de cumplimiento CT-CUM-R/A-2-2019, con base en lo cual se determina que se actualiza la causa de reserva prevista en el artículo 110, fracción VII, de la Ley Federal de Transparencia, ya que la divulgación de los datos referidos conllevaría un riesgo real, demostrable e identificable, en tanto que colocaría a la Suprema Corte de Justicia de la Nación en un estado de vulnerabilidad, facilitando el acceso ilícito a los equipos informáticos en materia de seguridad, intentando la suplantación de los mismos; potenciaría la posibilidad de vulnerar la seguridad de su infraestructura tecnológica; por tanto, pondría en un estado vulnerable a la institución.

En ese sentido, el perjuicio significativo al **interés público** resulta **menos restrictivo**, porque de lo contrario se pondría en riesgo la responsabilidad fundamental del Alto Tribunal en la defensa del orden establecido en la Constitución Federal, a través del ejercicio de sus funciones jurisdiccionales de orden constitucional, toda vez que difundir el nombre y la versión de la herramienta, aplicación, sistema o proceso de inteligencia artificial, para la automatización de las acciones de contención de eventos para la protección de los activos informáticos de la Suprema Corte de Justicia de la Nación, gestionadas por un Servicio Administrado de un Centro de Operaciones de Ciberseguridad, implicaría colocar en un estado de vulnerabilidad a este Alto Tribunal.

Acorde con las resoluciones a que se ha hecho referencia, el riesgo de perjuicio que supondría la divulgación supera el interés público

7O0pFAPhp5ZXGk3O3AgvT/mpeD17QD6U12ylATkfKBY=

general de que se difunda ese aspecto de la información solicitada, ya que la reserva de la información requerida en ese aspecto específico conlleva prevenir el delito de acceso ilícito a sistemas y equipos de informática tipificado en el Código Penal Federal, lo cual cobra importancia si se considera que dicha conducta implica conocer, copiar, modificar, destruir o provocar la pérdida de información contenida en sistemas o equipos de informática, por lo que revelar las marcas de los equipo utilizados para operar los servicios de seguridad informática de este Alto Tribunal *"no sólo se comprometería la información que obra en los archivos digitales del sujeto obligado, sino que menoscabaría la seguridad y certeza de los ciudadanos que acuden a éste para otorgar certeza respecto de la impartición de justicia y control constitucional".*

Ahora bien, dicha clasificación de reserva *"**se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio**"*, toda vez que **la pretensión de fondo que persigue la reserva de la información consiste en prevenir la conducta antijurídica tipificada** (acceso ilícito a sistemas y equipos de informática), de llevarse a cabo podría permitir la ejecución de diversos **ataques** a la infraestructura tecnológica y de sistemas con que cuenta este Alto Tribunal, ya que la difusión del nombre y versión de las herramientas con inteligencia artificial para la automatización de las acciones de contención de eventos para la protección de los activos informáticos de este Alto Tribunal, ***"incrementa sustancialmente la posibilidad de que aquella persona que conozca dicha información cometa algún ilícito"***, pues tendría acceso a información con un alto grado de precisión técnica y las características de la infraestructura instalada.

Plazo de reserva.

7O0pFAPhp5ZXGk3O3AgvT/mpeD17QD6U12ylATkfKBY=

Considerando lo argumentado en las resoluciones que se citan como precedentes en este caso específico, es posible que se haga un pronunciamiento al respecto, ya que en otras resoluciones se ha hecho análisis sobre información de naturaleza similar, sin que por ello se desconozca la obligación que prevé el artículo 100, último párrafo, de la Ley General de Transparencia, en relación con el 17, párrafo primero, del Acuerdo General de Administración 5/2015, respecto de que es competencia de la persona titular de la instancia que tiene bajo resguardo la información requerida, pronunciarse expresamente sobre la clasificación de la información y, en su caso, el plazo de reserva y los motivos que sostengan la clasificación y que superen la prueba de daño.

En el caso específico, en términos de lo señalado en el artículo 101, párrafo segundo, de la Ley General de Transparencia, se determina que el plazo de reserva sea por cinco años, ya que acorde con las consideraciones expuestas en este apartado, en concordancia con lo resuelto en el cumplimiento CT-CUM-R/A-2-2019 y en la resolución del INAI a que se ha hecho mención, se considera que dicho plazo es proporcional a la naturaleza y el grado de especificidad del tipo de información de que se trata.

3. Información pendiente.

Como se advierte de los antecedentes, la Unidad General de Transparencia requirió a la Coordinación de la Ponencia de la Ministra Ríos Farjat que se pronunciara respecto a la aplicación denominada Sor Juana, sin que a la fecha de esta resolución se haya recibido la respuesta.

En consecuencia, considerando que este órgano colegiado es competente para dictar las medidas necesarias para localizar la

7O0pFAPhp5ZXGk3O3AgvT/mpeD17QD6U12ylATkfKBY=

información, con apoyo en los artículos 44, fracción I, de la Ley General de Transparencia, 23, fracción I, y 37, del Acuerdo General de Administración 5/2015, por conducto de la Secretaría Técnica de este Comité, se requiere a la Coordinación de la Ponencia de la Ministra Ana Margarita Ríos Farjat, para que remita a la Unidad General de Transparencia el informe que le fue solicitado, en el que se pronuncie sobre la existencia y disponibilidad de la información que da origen a este asunto, respecto de la referida aplicación, sin perjuicio de que esa unidad general someta a consideración de este Comité de Transparencia, dicha respuesta, si del contenido de ese informe se actualiza la competencia de este órgano colegiado.

Por lo expuesto y fundado, se

R E S U E L V E:

PRIMERO. Se tiene por atendida la solicitud, respecto de la información abordada en el apartado 1 de la consideración segunda de la presente resolución.

SEGUNDO. Se confirma la clasificación como reservada de la información a que se hace referencia en el apartado 2 de la segunda consideración de esta determinación.

TERCERO. Se requiere a la Coordinación de la Ponencia de la Ministra Ríos Farjat, en los términos expuestos en el apartado 3, del último considerando de la presente determinación.

7O0pFAPhp5ZXGk3O3AgvT/mpeD17QD6U12ylATkfKBY=

CUARTO. Se requiere a la Unidad General de Transparencia, para que realice las acciones señaladas en esta resolución.

Notifíquese a la persona solicitante, a las instancias vinculadas y a la Unidad General de Transparencia.

Por unanimidad de votos lo resolvió el Comité de Transparencia de la Suprema Corte de Justicia de la Nación, integrado por el licenciado Mario José Pereira Meléndez, Director General de Asuntos Jurídicos y Presidente del Comité, maestro Christian Heberto Cymet López Suárez, Contralor del Alto Tribunal, y licenciado Adrián González Utusástegui, Titular de la Unidad General de Investigación de Responsabilidades Administrativas; quienes firman con la secretaria del Comité que autoriza.

LICENCIADO MARIO JOSÉ PEREIRA MELÉNDEZ
PRESIDENTE DEL COMITÉ

MAESTRO CHRISTIAN HEBERTO CYMET LÓPEZ SUÁREZ
INTEGRANTE DEL COMITÉ

LICENCIADO ADRIÁN GONZÁLEZ UTUSÁSTEGUI
INTEGRANTE DEL COMITÉ

MAESTRA SELENE GONZÁLEZ MEJÍA
SECRETARIA DEL COMITÉ

"Resolución formalizada por medio de la Firma Electrónica Certificada del Poder Judicial de la Federación (FIREL), con fundamento en los artículos tercero y quinto del Acuerdo General de Administración III/2020 del Presidente de la Suprema Corte de Justicia de la Nación, de diecisiete de septiembre de dos mil veinte, en relación con la RESOLUCIÓN adoptada sobre el particular por el Comité de Transparencia de la Suprema Corte de Justicia de la Nación en su Sesión Ordinaria del siete de octubre de dos mil veinte."

7O0pFAPhp5ZXGk3O3AgvT/mpeD17QD6U12ylATkfKBY=