



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

VARIOS CT-VT/A-8-2025

INSTANCIA VINCULADA:

DIRECCIÓN GENERAL DE
TECNOLOGÍAS DE LA
INFORMACIÓN

Ciudad de México. Resolución del Comité de Transparencia de la Suprema Corte de Justicia de la Nación, correspondiente al **veintiséis de marzo de dos mil veinticinco**.

ANTECEDENTES:

PRIMERO. Solicitud de información. El veinticinco de febrero de dos mil veinticinco, se recibió la solicitud registrada en la Plataforma Nacional de Transparencia con el folio 330030525000346, en cuyo anexo se pidió lo siguiente:

*“Estimado equipo de la SCJN,
Actualmente estoy trabajando en un proyecto que requiere la integración con los servicios ofrecidos por la plataforma del Semanario Judicial de la Federación (SJF). Hemos identificado algunos endpoints públicos, como los siguientes:*

- <https://sjf2.scjn.gob.mx/services/sjftesismicroservice/api/public/Ley>*
- <https://sjf2.scjn.gob.mx/services/sjftesismicroservice/api/public/tesis>*

Sabemos que la API permite realizar consultas avanzadas sobre tesis y obtener detalles específicos utilizando clasificadores, operadores lógicos y expresiones compuestas. Sin embargo, para realizar una integración eficiente y aprovechar al máximo sus funcionalidades, agradecería si pudieran proporcionarme la documentación técnica completa de la API.

Con fundamento en el artículo 8 constitucional, de manera pacífica y respetuosa, solicito la siguiente información:

1. Documentación general de la API:

- Alcance y funcionalidades principales del microservicio de tesis.*
- Detalles sobre autenticación, autorización y cualquier medida de seguridad aplicable.*
- Políticas de uso, límites de consultas (rate limits) y consideraciones legales.*

2. Catálogo completo de Endpoints disponibles:

- Descripción de todos los endpoints disponibles (GET, POST, PUT, DELETE), incluyendo entre otros: 1) Búsqueda avanzada de tesis mediante clasificadores y operadores lógicos; 2) Obtención de detalles específicos de una tesis*

8vXL8GUquwpXBQxhZFLvuhv1/aC3qbtucG6RhIMLoQ=

utilizando la clave IUS; 3) Consulta de leyes, artículos y reformas legales; 4) Parámetros requeridos y opcionales para cada endpoint; 5) Ejemplos de peticiones y respuestas esperadas.

3. Estructura de datos y catálogos:

- Explicación detallada de campos como idLey, idReforma, idArticulo y ius.*
- Información sobre clasificadores utilizados en las búsquedas avanzadas (ej. idEpoca, materia, etc.).*
- Métodos disponibles para obtener catálogos de leyes, artículos, épocas, materias y otras entidades relacionadas.*

4. Manejo de errores y respuestas:

- Códigos de estado HTTP utilizados por la API.*
- Mensajes de error comunes y recomendaciones para su tratamiento.*
- Buenas prácticas para el control de errores y manejo de respuestas vacías.*

5. Recomendaciones y buenas prácticas:

- Reglas y sugerencias para realizar consultas optimizadas y eficientes.*
- Restricciones técnicas o legales a considerar durante la integración.”*

SEGUNDO. Acuerdo de admisión de la solicitud. En acuerdo de veinticinco de febrero 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 Ley Federal de Transparencia y Acceso a la Información Pública (Ley Federal de Transparencia) y 7 del Acuerdo General de Administración 5/2015, la estimó procedente y ordenó abrir el expediente UT/A/0087/2025.

TERCERO. Requerimiento de información. Mediante oficio UGTSIJ/TAIPDP-526-2025 del titular de la Unidad General de Transparencia, enviado por el Sistema de Gestión Documental Institucional el veintiséis de febrero de dos mil veinticinco, se solicitó a la Dirección General de Tecnologías de la Información (DGTI) que se pronunciara sobre la información solicitada y, en su caso, sobre su clasificación.



CUARTO. Solicitud de prórroga de DGTI. Mediante correo electrónico de cinco de marzo de dos mil veinticinco dirigido a la Unidad General de Transparencia, la instancia referida solicitó un plazo adicional para responder al requerimiento.

QUINTO. Informe de DGTI. Mediante oficio DGTI/134/2025 de diez de marzo de dos mil veinticinco, el área vinculada rindió el informe que le fue solicitado en el sentido siguiente:

“(…)

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 proporciona vínculo electrónico para consulta), a través de la Subdirección General de Desarrollo 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 cuanto al numeral 1 en la parte en la que se requiere: Alcance y funcionalidades principales del microservicio de tesis, en primer lugar, se precisa que no existe obligación de la Dirección General de Tecnologías de la Información para generar un documento ad hoc, con base en el Criterio reiterado y vigente [SO/003/2017](#) (del que se inserta vínculo electrónico de consulta), emitido por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, denominado ‘No existe obligación de elaborar documentos ad hoc para atender las solicitudes de acceso a la información’. No obstante lo anterior, en aras del principio de máxima publicidad se informa que el alcance y funcionalidades son los siguientes:

Alcance:

Fue elaborado para difundir información mensual y semanal de las tesis en los módulos del Semanario Judicial de la Federación (Semanal, Sistematizado y eGaceta).

Funcionalidades:

Consulta de listado de tesis por palabra o frase, consulta de listado de tesis por palabra o frase exacta, consulta de listado de tesis por palabras o frases concatenadas por operadores lógicos, consulta de listado de tesis por números de Registro Digital (IUS), consulta de listado de tesis por clasificadores dinámicos (época, año, instancia, órgano, materia, asunto, ponente), consulta del detalle de la tesis, consulta de documentos asociados a la tesis, consulta de anexos de la tesis, consulta de listado de tesis por tema, consulta de listado de jurisprudencia histórica, consulta a legislaciones estatales y/o federales

mediante ligas, descarga de listado de resultados de tesis en PDF, descarga del detalle de la tesis en PDF.

Es importante precisar que el microservicio de tesis se encuentra inmerso en el Sistema de Consulta del Semanario Judicial de la Federación (del que se inserta liga electrónica), y puede ser consultado por cualquier persona.

Al dar clic en el vínculo antes citado, se pueden visualizar cuatro secciones para realizar consultas sobre:

- *Tesis, precedentes (sentencias) y otros documentos publicados semanalmente.*
- *Sistematización de tesis publicadas en el Semanario Judicial de la Federación de 1917 a la fecha.*
- *Precedentes (incluye controversias, acciones y declaratorias)*
- *Gaceta.*

Asimismo, se pueden visualizar las funcionalidades adicionales, como:

- *Normativa del Semanario Judicial de la Federación.*
- *Listados obligatorios previstos en el Acuerdo General 17/19.*
- *Manual de usuario.*
- *Galería virtual del Semanario Judicial de la Federación.*

Ahora bien, respecto a la porción del numeral 1 de la solicitud en donde se requieren detalles sobre políticas de uso, límites de consultas (rate limits) y consideraciones legales, la parte del numeral 4 que refiere buenas prácticas para el control de errores y manejo de respuestas vacías), así como el numeral 5 que refiere recomendaciones y buenas prácticas, reglas y sugerencias para realizar consultas optimizadas y eficientes, restricciones técnicas o legales a considerar durante la integración, se informa que no se cuenta con dicha información, por lo que resulta aplicable el Criterio reiterado y vigente SO/007/2017 (del que se inserta liga electrónica) emitido por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, denominado 'Casos en los que no es necesario que el Comité de Transparencia confirme formalmente la inexistencia de la información'.

En cuanto a la porción del numeral 1 que señala autenticación, autorización y cualquier medida de seguridad aplicable, así como a los numerales 2, 3 y 4 en los que se requiere, respectivamente: 2. Catálogo completo de Endpoints disponibles: (Descripción de todos los endpoints disponibles (GET, POST, PUT, DELETE), incluyendo entre otros: 1) Búsqueda avanzada de tesis mediante clasificadores y operadores lógicos; 2) Obtención de detalles específicos de una tesis utilizando la clave IUS; 3) Consulta de leyes, artículos y reformas legales; 4) Parámetros requeridos y opcionales para cada endpoint; 5) Ejemplos de peticiones y respuestas esperadas; 3. Estructura de datos y catálogos: (Explicación detallada de campos como idLey, idReforma, idArticulo y ius. Información sobre clasificadores utilizados en las búsquedas avanzadas (ej. idEpoca, materia, etc.). Métodos disponibles para obtener catálogos de leyes, artículos, épocas, materias y otras entidades relacionadas; y 4. Manejo de errores y respuestas: (Códigos de estado HTTP utilizados por la API. Mensajes de error comunes y recomendaciones para su tratamiento).



Sobre el particular, se informa que la información solicitada se considera reservada, conforme a los artículos 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP), de la que se inserta vínculo electrónico de consulta y 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP) de la que se proporciona vínculo electrónico.

Mismos que señalan en su fracción VII, lo siguiente:

‘VII Obstruya la prevención o persecución de los delitos;’.

Considerando que una API o Interfaz de Programación de Aplicaciones (Application Programming Interface), es un conjunto de reglas y protocolos que permiten que diferentes aplicaciones de software se comuniquen e intercambien datos entre sí, operando como un intermediario que facilita la interacción entre dos sistemas, permitiéndoles compartir información y funcionalidades, y en virtud de la naturaleza, así como el grado de especificidad del tipo de información que se requiere, es que se realiza la siguiente prueba de daño:

- La difusión de la información llevaría 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 la infraestructura tecnológica del propio sistema, ya que potenciaría la posibilidad de vulnerar la seguridad de su infraestructura tecnológica, y podría poner en riesgo cuestiones de seguridad de informática.*
- Difundir información sobre la autenticación y autorización colocaría a la Suprema Corte de Justicia de la Nación en un estado de vulneración al permitir que diversos entes puedan acceder al uso directo de la API, sin realizarlo a través del propio sistema del Semanario Judicial de la Federación, poniendo en riesgo la operación del propio sistema, o en su caso, de la infraestructura tecnológica de la Suprema Corte de Justicia de la Nación.*
- Proporcionar los detalles relacionados con los endpoints, pueden ocasionar un consumo inapropiado de la infraestructura tecnológica de la Suprema Corte de Justicia de la Nación, causando una degradación del servicio que brinda el Semanario Judicial de la Federación.*
- Compartir la estructura de datos y catálogos, así como manejo de errores y respuestas, o cualquier otra información relacionada con la infraestructura tecnológica o de la arquitectura del propio Semanario Judicial de la Federación, conllevaría a posible estado de vulnerabilidad, ya que dichos detalles pueden ser utilizados de manera inadecuada, retrasando o impidiendo la difusión de las tesis y jurisprudencia, teniendo un impacto negativo en el acceso a la justicia.*
- En este sentido, permitiría que cualquier persona experta en la materia, le dé el uso que mejor le convenga y pueda vulnerar la seguridad de la infraestructura tecnológica de la Suprema Corte de Justicia de la Nación, ya que con la información al grado de detalle que la requiere, se le daría a conocer la arquitectura tecnológica del Semanario Judicial de la Federación, facilitando el posible acceso ilícito a la infraestructura tecnológica del propio sistema y podría poner en riesgo cuestiones de seguridad informática, exponiendo la capacidad de reacción ante posibles ataques informáticos.*

- *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 por el solicitante implica 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, particularmente en los correspondientes a seguridad informática.*
- *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 de información de la arquitectura o diseño del Semanario Judicial de la Federación, 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.*

Derivado de todo lo anterior, cabe preciar que el Código Penal Federal (del que se inserta vínculo electrónico para consulta), dispone lo siguiente:

‘Acceso ilícito 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 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.

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.'

De los preceptos antes citados, se advierte que 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, 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 la información podría ocasionar lo siguiente:

- Colocaría a la Suprema Corte de Justicia de la Nación en un estado de vulnerabilidad, facilitando el acceso ilícito a la infraestructura tecnológica del propio sistema.*
- Potenciaría la posibilidad de vulnerar la seguridad de su infraestructura tecnológica.*
- Pondría en un estado vulnerable a la institución.*
- Podría poner en riesgo cuestiones de seguridad informática o de operación del sistema.*

Ahora bien, en cuanto al periodo de reserva, el artículo 99 de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el Trigésimo Cuarto de los Lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, (de los que se inserta vínculo electrónico), establecen que la información clasificada podrá permanecer con tal carácter, hasta por un periodo de cinco años, y que tal información podrá ser desclasificada: a) cuando se extingan las causas que dieron origen a su clasificación; b) cuando expire el plazo de clasificación; c) cuando exista resolución de una autoridad competente que determine que existe una causa de interés público que prevalece sobre la reserva de la información; d) cuando el Comité de Transparencia considere pertinente la desclasificación de conformidad con el Título cuarto del mismo ordenamiento, o e) cuando se trate de información que esté relacionada con violaciones graves a derechos humanos o delitos de lesa humanidad.

En el caso concreto, considerando que el bien jurídico tutelado es la seguridad de los sistemas y equipos de informática, se considera que el periodo de reserva debe ser de 5 años.

Por último, sirve como precedente, lo resuelto por el Comité de Transparencia de la Suprema Corte de Justicia de la Nación, a través de la resolución del expediente CT-CI/A-55-2023 (del que se inserta vínculo electrónico de consulta), en donde se analiza la causal de reserva invocada en el presente asunto."

SEXTO. Vista a la Secretaría del Comité de Transparencia.

Mediante correo electrónico de catorce de marzo de dos mil veinticinco, la Unidad General de Transparencia remitió el oficio UGTSIJ/TAIPDP-657-2025 y el expediente electrónico UT-A/0087/2025 a la Secretaría del Comité de Transparencia.

SÉPTIMO. Acuerdo de turno. En acuerdo de dieciocho de marzo de dos mil veinticinco, con fundamento en los artículos 44, fracción II, de la entonces vigente 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-8-2025** y, conforme al turno correspondiente, remitirlo a la Unidad General de Investigación de Responsabilidades Administrativas, lo que se hizo mediante oficio CT-80-2025, enviado por correo electrónico en la misma fecha.

CONSIDERACIONES:

PRIMERA. Competencia. 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 lo dispuesto en 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, 65, fracciones I y II, de la Ley Federal de Transparencia, así como 23, fracciones I y II, del Acuerdo General de Administración 5/2015.

Cabe resaltar que por decreto publicado en el Diario Oficial de la Federación el veinte de marzo de dos mil veinticinco, el cual entró en vigor al día siguiente, se expidieron entre otras, la Ley General de Transparencia y Acceso a la Información Pública, y a la entrada en vigor



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

VARIOS CT-VT/A-8-2025

de ese decreto, atento a su artículo transitorio segundo, se abrogaron entre otras, la Ley General de Transparencia y Acceso a la Información Pública, publicada en el Diario Oficial de la Federación el cuatro de mayo de dos mil quince y sus modificaciones posteriores, así como la Ley Federal de Transparencia y Acceso a la Información Pública, publicada en el Diario Oficial de la Federación el nueve de mayo de dos mil dieciséis y sus modificaciones posteriores.

Sin embargo, el régimen transitorio del referido decreto no prevé qué disposiciones habrán de regir para la atención de solicitudes de acceso a la información de los actuales sujetos obligados del Poder Judicial de la Federación, como es esta Suprema Corte de Justicia de la Nación.

En ese sentido, se considera que para 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, aplican por identidad jurídica las mismas razones previstas en el artículo transitorio noveno del mencionado decreto, el cual dispone en la parte conducente, que los procedimientos iniciados con anterioridad a la entrada en vigor del decreto ante al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, en materia de acceso a la información pública, se sustanciarán conforme a las disposiciones aplicables vigentes al momento de su inicio.

Por tanto, ya que la solicitud que se atiende fue presentada a través de la Plataforma Nacional de Transparencia (PNT) el veinticinco de febrero de dos mil veinticinco, se estima resultan aplicables al caso las disposiciones vigentes hasta antes de la entrada en vigor del mencionado decreto.

8vXL8GUquwpXBQxhZF/Lvuhv1/aC3qbtucG6RhIMLoQ=

SEGUNDA. Análisis. En la solicitud se pide diversa información relativa a la API¹ (por sus iniciales en inglés Interfaz de Programación de Aplicaciones) del micrositio de tesis de este Alto Tribunal relativa a los cuatro rubros siguientes:

1. Documentación General
2. Catálogo completo de *Endpoints* disponibles
3. Estructura de datos y catálogos
4. Manejo de errores y respuestas
5. Recomendaciones y buenas prácticas.

Al respecto la Dirección General de Tecnologías de la Información se pronunció en el sentido siguiente:

Solicitud	Respuesta
1. <i>Documentación general de la API:</i>	No existe la obligación de elaborar un documento ad hoc pero se proporciona la información:
• <i>Alcance y funcionalidades principales del microservicio de tesis.</i>	Alcance: <i>Fue elaborado para difundir información mensual y semanal de las tesis en los módulos del Semanario Judicial de la Federación (Semanal, Sistematizado y eGaceta).</i> Funcionalidades: <i>Consulta de listado de tesis por palabra o frase, consulta de listado de tesis por palabra o frase exacta, consulta de listado de tesis por palabras o frases concatenadas por operadores lógicos, consulta de listado de tesis por números de Registro Digital (IUS), consulta de listado de tesis por clasificadores dinámicos (época, año, instancia, órgano, materia, asunto, ponente), consulta del detalle de la tesis, consulta de documentos asociados a la tesis, consulta de anexos de la tesis, consulta de listado de tesis por tema, consulta de listado de jurisprudencia histórica, consulta a legislaciones estatales y/o federales mediante ligas, descarga de</i>

¹ Application Programing Interface.



	<i>listado de resultados de tesis en PDF, descarga del detalle de la tesis en PDF. Es importante precisar que el microservicio de tesis se encuentra inmerso en el Sistema de Consulta del Semanario Judicial de la Federación (del que se inserta liga electrónica), y puede ser consultado por cualquier persona. Al dar clic en el vínculo antes citado, se pueden visualizar cuatro secciones para realizar consultas sobre:</i> <i>• Tesis, precedentes (sentencias) y otros documentos publicados semanalmente.</i> <i>• Sistematización de tesis publicadas en el Semanario Judicial de la Federación de 1917 a la fecha.</i> <i>• Precedentes (incluye controversias, acciones y declaratorias)</i> <i>• Gaceta.</i> <i>Asimismo, se pueden visualizar las funcionalidades adicionales, como:</i> <i>• Normativa del Semanario Judicial de la Federación.</i> <i>• Listados obligatorios previstos en el Acuerdo General 17/19.</i> <i>• Manual de usuario.</i> <i>• Galería virtual del Semanario Judicial de la Federación.</i>
<i>• Detalles sobre autenticación, autorización y cualquier medida de seguridad aplicable.</i>	Reservada
<i>• Políticas de uso, límites de consultas (rate limits) y consideraciones legales.</i>	No se cuenta con dicha información
<i>2. Catálogo completo de Endpoints disponibles:</i> <i>• Descripción de todos los endpoints disponibles (GET, POST, PUT, DELETE), incluyendo entre otros:1) Búsqueda avanzada de tesis mediante clasificadores y operadores lógicos; 2) Obtención de detalles específicos de una tesis utilizando la clave IUS; 3) Consulta de leyes, artículos y reformas legales; 4) Parámetros requeridos y opcionales para cada endpoint; 5) Ejemplos de peticiones y respuestas esperadas.</i>	Reservada

8vXL8GUquwpXBQxhZFLvuhv1/aC3qbtucG6RhIMLoQ=

3. Estructura de datos y catálogos: • Explicación detallada de campos como <i>idLey</i>, <i>idReforma</i>, <i>idArticulo</i> y <i>ius</i>. • Información sobre clasificadores utilizados en las búsquedas avanzadas (ej. <i>idEpoca</i>, <i>materia</i>, etc.). • Métodos disponibles para obtener catálogos de leyes, artículos, épocas, materias y otras entidades relacionadas.	Reservada
4. Manejo de errores y respuestas: • Códigos de estado HTTP utilizados por la API. • Mensajes de error comunes y recomendaciones para su tratamiento.	Reservada
• Buenas prácticas para el control de errores y manejo de respuestas vacías	No se cuenta con dicha información
5. Recomendaciones y buenas prácticas: • Reglas y sugerencias para realizar consultas optimizadas y eficientes. • Restricciones técnicas o legales a considerar durante la integración.”	No se cuenta con dicha información

Establecido lo anterior, este Comité determina lo siguiente:

1. Información que se pone a disposición.

En lo que concierne a la información solicitada en el punto 1 (alcances y funcionalidades de la *API*) la DGTI, en principio, señala que no cuenta con la obligación de generar un documento *ad hoc*; sin embargo, proporciona el alcance y funcionalidades.

Al respecto, con lo señalado por el área vinculada se tiene por atendido ese punto.

Por consiguiente, se instruye a la Unidad General de Transparencia que ponga a disposición de la persona solicitante la información proporcionada por la DGTI.

2. Información reservada.



En lo que concierne a lo solicitado en el penúltimo punto del apartado 1 (detalles sobre autenticación, autorización y cualquier medida de seguridad aplicable), la totalidad de los puntos requeridos en los apartados 2 y, 3, así como 4 en los dos primeros puntos (código de estado *HTTP* utilizado por la *API*, mensajes de error comunes y recomendaciones para su tratamiento); la DGTI clasifica la información como reservada en términos de lo dispuesto en el artículo 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública y 113, fracción VII, de la Ley General de Transparencia y Acceso a la Información Pública, entonces vigentes.

Lo anterior en virtud de que la *API* o Interfaz de Programación de Aplicaciones, es un conjunto de reglas y protocolos que permiten que diferentes aplicaciones de *software* se comuniquen o intercambien datos entre sí, operando como un intermediario que facilita la interacción entre dos sistemas, que posibilita compartir información y funcionalidad.

Por lo que, atendiendo a la naturaleza y grado de especialidad de la información que se requiere, la DGTI estima que su difusión implica un riesgo real, demostrable e identificable, en tanto que colocaría a la Suprema Corte de Justicia de la Nación en un estado de vulnerabilidad,

Para emitir pronunciamiento sobre la clasificación de la información que se anunció, se tiene en cuenta que, efectivamente, este Comité al resolver el asunto CT-VT/A-39-2022 sostuvo 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 encuentra acotado en función de ciertas causas e intereses relevantes, así como frente al necesario tránsito de las vías adecuadas para ello².

En atención a la disposición constitucional referida, la información que tienen bajo resguardo los sujetos obligados del Estado es pública y solo encuentra como excepción aquella que sea temporalmente reservada o confidencial en los términos establecidos por el legislador federal o local.

Ahora bien, para sustentar la reserva de la información, la instancia vinculada señala que la divulgación la información solicitada conllevaría a un riesgo real, demostrable e identificable en virtud de que:

- Facilitaría el acceso ilícito a la infraestructura tecnológica del propio sistema, en tanto que potencializaría la posibilidad de vulnerar la seguridad de su infraestructura tecnológica, y pondría en riesgo las cuestiones de seguridad informática de este Alto Tribunal.

² **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. 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.



- Difundiría información sobre la autenticación y autorización de la *API*, colocaría a este Máximo Tribunal en un estado de vulnerabilidad al permitir que diversos entes puedan acceder al uso directo de esa *API*, sin que deban realizarlo a través del propio sistema del Semanario Judicial de la Federación, lo que pondría en riesgo la operación del propio sistema, o en su caso, de la infraestructura tecnológica de la Suprema Corte de Justicia de la Nación.
- Proporcionar los detalles relacionados con los *endpoints*, pueden ocasionar un consumo inapropiado de la infraestructura tecnológica de la Suprema Corte de Justicia de la Nación, causando una degradación del servicio que brinda el Semanario Judicial de la Federación.
- Compartir la estructura de datos y catálogos, así como manejo de errores y respuestas, o cualquier otra información relacionada con la infraestructura tecnológica o de la arquitectura del propio Semanario Judicial de la Federación, conllevaría a un posible estado de vulnerabilidad, ya que dichos detalles pueden ser utilizados de manera inadecuada, retrasando o impidiendo la difusión de las tesis y jurisprudencia, teniendo un impacto negativo en el acceso a la justicia
- Permitiría que cualquier persona experta en la materia, le dé el uso que mejor le convenga y pueda vulnerar la seguridad de la infraestructura tecnológica de la Suprema Corte de Justicia de la Nación, ya que con la información al grado de detalle que se requiere, como se mencionó, se daría a conocer la arquitectura tecnológica del Semanario Judicial de la Federación, facilitando el posible acceso ilícito a la

infraestructura tecnológica del propio sistema y podría poner en riesgo cuestiones de seguridad informática, exponiendo la capacidad de reacción ante posibles ataques informáticos.

Como se señaló, la reserva de la información se fundamentó en el artículo 110, fracción VII, de la Ley Federal³ de Transparencia y 113, fracción VII, de la Ley General de Transparencia⁴, entonces vigentes, bajo el argumento de que su divulgación pondría en riesgo la seguridad de la infraestructura tecnológica de este Alto Tribunal y expondría la capacidad de reacción ante posibles ataques informáticos, además de que propiciaría la degradación del servicio que brinda la *API*, pues podría ser utilizada la información de manera inadecuada, retrasando o impidiendo la difusión de las tesis y jurisprudencia.

Los artículos referidos disponen que como información reservada podrá clasificarse aquella cuya publicación pueda causar daño u obstruya la prevención o persecución del delito.

En relación con lo anterior, es posible tener presente lo resuelto por el entonces Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales en el recurso de revisión PRA-10276/18, cumplimentado por este Comité en la resolución CT-CUM-R/A-2-2019, ya que se determinó 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**

³ “**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;

(...)

⁴ “**Artículo 113.** Como información reservada podrá clasificarse aquella cuya publicación:

(...)

VII. Obstruya la prevención o persecución de los delitos;

(...)”



autoridades para evitar su comisión, o menoscabar o limitar la capacidad de las autoridades para evitar la 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)

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 (que fue retomado en la resolución CT-VT/A-39-2022), este Comité de Transparencia **confirma la reserva** de los datos requeridos en penúltimo punto del apartado 1 (detalles sobre autenticación, autorización y cualquier medida de seguridad aplicable), la totalidad de los puntos requeridos en los apartados 2, 3, así como 4 en los dos primeros puntos (código de estado *HTTP* utilizado por la *API*, mensajes de error comunes y recomendaciones para su tratamiento), con fundamento en el artículo 113, fracción VII, de la Ley General de Transparencia.

Lo anterior es así, dado que, la DGTI 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.



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 DGTI, así como lo argumentado en la resolución del INAI en el recurso de revisión RRA 10276/18 y la resolución de cumplimiento CT-CUM-R/A-2-2019, con base en lo cual se determina que se actualiza la causal 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 información sobre la autenticación y autorización de la *API*, proporcionar los detalles relacionados con los *endpoints*, compartir la estructura de datos y catálogos, así como manejo de errores y respuestas, así como cualquier otra información relacionada con la infraestructura tecnológica o de la arquitectura del propio Seminario Judicial de la Federación, conllevaría un estado de vulnerabilidad la información de 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 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 la información solicitada en el penúltimo punto del apartado 1 (detalles sobre autenticación, autorización y cualquier medida de seguridad aplicable), la totalidad de los puntos requeridos en los apartados 2, 3, así como 4 en los dos primeros puntos (código de estado *HTTP* utilizado por la *API*, mensajes de error comunes y recomendaciones para su tratamiento) *“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 de información solicitada, ***“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, así como a los protocolos de seguridad y las características de la infraestructura instalada.

Plazo de reserva.



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 Transparencia⁵, en relación con el 17, párrafo primero, del Acuerdo General de Administración 5/2015⁶, 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, los motivos que sustenten la prueba de daño y, el plazo de reserva.

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 inexistente.

En relación con lo solicitado en el último punto del apartado 1, último punto del apartado 4 y apartado 5, la DGTI informó no contar con dicha información.

⁵ “**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.”

⁶ “**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. [...]”

Sobre la inexistencia anunciada, se recuerda que el derecho de acceso a la información pública comprende solicitar, investigar, difundir, buscar y recibir información, que se encuentre integrada en documentos que registren el ejercicio de las facultades, funciones y competencias de los sujetos obligados, lo que vincula a las dependencias y entidades a documentar todo lo relativo a éstas y presume su existencia de conformidad con lo establecido en los artículos 3, fracción VII, 4, 18 y 19, de la Ley General de Transparencia⁷.

Enseguida, se debe destacar que de conformidad con el artículo 36, fracciones I, V, VIII y IX, del Reglamento Orgánico en Materia de Administración⁸, de la Suprema Corte de Justicia de la Nación, a la Dirección General de Tecnologías de la Información le corresponde:

⁷ “**Artículo 3.** Para los efectos de la presente Ley se entenderá por: [...]”

VII. Documento: Los expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas o bien, cualquier otro registro que documente el ejercicio de las facultades, funciones y competencias de los sujetos obligados, sus Servidores Públicos e integrantes, sin importar su fuente o fecha de elaboración. Los documentos podrán estar en cualquier medio, sea escrito, impreso, sonoro, visual, electrónico, informático u holográfico; [...]”

“**Artículo 4.** El derecho humano de acceso a la información comprende solicitar, investigar, difundir, buscar y recibir información. Toda la información generada, obtenida, adquirida, transformada o en posesión de los sujetos obligados es pública y accesible a cualquier persona en los términos y condiciones que se establezcan en la presente Ley, en los tratados internacionales de los que el Estado mexicano sea parte, la Ley Federal, las leyes de las Entidades Federativas y la normatividad aplicable en sus respectivas competencias; sólo podrá ser clasificada excepcionalmente como reservada temporalmente por razones de interés público y seguridad nacional, en los términos dispuestos por esta Ley.”

“**Artículo 18.** Los sujetos obligados deberán documentar todo acto que derive del ejercicio de sus facultades, competencias o funciones.”

“**Artículo 19.** Se presume que la información debe existir si se refiere a las facultades, competencias y funciones que los ordenamientos jurídicos aplicables otorgan a los sujetos obligados. En los casos en que ciertas facultades, competencias o funciones no se hayan ejercido, se debe motivar la respuesta en función de las causas que motiven la inexistencia.”

⁸ “**Artículo 36.** La Dirección General de Tecnologías de la Información tendrá las atribuciones siguientes: I, Administrar los recursos en materia de tecnologías de la información y comunicación, así como proveer los servicios que se requieran en la materia; [...] V. Planificar, diseñar, desarrollar y mantener en operación los sistemas informáticos jurídicos, administrativos y jurisdiccionales, así como los portales y microsítios que requieran los órganos y áreas, de conformidad con las disposiciones jurídicas aplicables; [...]”



- administrar los recursos en materia de tecnologías de la información y comunicación y proveer los servicios que se requieran en la materia;
- planear, diseñar mantener y supervisar la operación de los sistemas informáticos jurídicos, administrativos y jurisdiccionales, así como los portales y micrositios que requieran los órganos y áreas;
- proporcionar los servicios de mantenimiento a las redes, sistemas, equipo informático, comunicación y digitalización de los órganos y áreas de este Alto Tribunal y, en su caso, a otros órganos del Poder Judicial de la Federación;
- instrumentar los mecanismos en materia de seguridad informática y vigilar su adecuado funcionamiento;
- atender las necesidades tecnológicas en materia de informática jurídica, así como desarrollar los programas informáticos que se utilizan en este Alto Tribunal.

En ese sentido, si la DGTI informó no contar con la información referida en el presente considerando, ya que es el área competente para pronunciarse sobre dicha información, se estima que no se está en el supuesto previsto en la fracción I del artículo 138 de la Ley General de Transparencia⁹ conforme al cual deban dictarse otras medidas para

⁹ “**Artículo 138.** Cuando la información no se encuentre en los archivos del sujeto obligado, el Comité de Transparencia:

I. Analizará el caso y tomará las medidas necesarias para localizar la información;

II. Expedirá una resolución que confirme la inexistencia del Documento;

III. Ordenará, siempre que sea materialmente posible, que se genere o se reponga la información en caso de que ésta tuviera que existir en la medida que deriva del ejercicio de sus facultades, competencias o funciones, o que previa acreditación de la imposibilidad de su generación, exponga de forma fundada y motivada, las razones por las cuales en el caso particular no ejerció dichas facultades, competencias o funciones, lo cual notificará al solicitante a través de la Unidad de Transparencia, y

IV. Notificará al órgano interno de control o equivalente del sujeto obligado quien, en su caso, deberá iniciar el procedimiento de responsabilidad administrativa que corresponda.”

localizar la información, pues se trata del área que podría contar con información de esa naturaleza, pero ha señalado que no tiene la información solicitada que se refiere en el presente considerando.

Además, tampoco se está en el supuesto de exigirle que genere la información que se pide conforme lo prevé la fracción III del citado artículo 138 de la Ley General, porque no se advierte atribución para contar con dicha información, de ahí que se confirma la inexistencia de lo solicitado en el último punto del apartado 1, último punto del apartado 4 y apartado 5, pues la DGTI informó no contar con dicha información, sin que ello constituya una restricción al derecho de acceso a la información.

Por lo expuesto y fundado; se,

R E S U E L V E:

PRIMERO. Se tiene por atendida la solicitud, de acuerdo con lo precisado en el considerando 1 de la presente determinación.

SEGUNDO. Se confirma la clasificación como información reservada en términos de lo precisado en el considerando 2 de esta determinación.

TERCERO. Se confirma la inexistencia de la información a que se hace referencia en el apartado 3 de esa determinación.

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

Notifíquese a la persona solicitante, a la instancia vinculada y a la Unidad General de Transparencia.



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

VARIOS CT-VT/A-8-2025

Así, por unanimidad de votos, lo resolvió el Comité de Transparencia de la Suprema Corte de Justicia de la Nación y firman el Licenciado Mario José Pereira Meléndez, Director General de Asuntos Jurídicos y Presidente del Comité; el Maestro Christian Heberto Cymet López Suárez, Contralor del Alto Tribunal; y, el Licenciado Adrián González Utusástegui, Titular de la Unidad General de Investigación de Responsabilidades Administrativas; integrantes del Comité, ante la Secretaria del Comité, quien autoriza y da fe.

**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.”

AGU/kmo