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

CUMPLIMIENTO CT-CUM/A-6-2026, DERIVADO DEL DIVERSO CT-CI/A-2-2021

INSTANCIA RESPONSABLE:

- 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 **doce de febrero de dos mil veintiséis.**

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

PRIMERO. Solicitud de información. El cuatro de enero de dos mil veintiuno, se recibió la solicitud de acceso a la información registrada en la Plataforma Nacional de Transparencia con el folio **0330000000221**, en la que se pidió lo siguiente:

> "Con base en mi derecho a la información y en versión pública, solicito conocer el número total de ataques cibernéticos que registró la institución, del 1 de enero de 2020 a la fecha. Favor de detallar por ataques totales, tipo de ataque, país de procedencia, tipo de afectación y si se levantó alguna denuncia penal, y en su caso, si hubo algún detenido" (sic)

SEGUNDO. Resolución del Comité de Transparencia en la que se clasificó la información: En sesión de veintisiete de enero de dos mil veintiuno, el Comité de Transparencia de la Suprema Corte de Justicia de la Nación (en lo sucesivo Comité de Transparencia), resolvió el expediente **CT-CI/A-2-2021**[1], en la cual determinó, en la parte que interesa, lo siguiente:

> " […]
> **II. Información reservada.**
>
> Por cuanto a lo requerido sobre el tipo de ataque y país de procedencia mencionados en el punto 2, en la nota del Director de Seguridad Informática y del Jefe de Departamento de Criptografía y Autentificación se clasifica dicha información como reservada, haciendo referencia a la resolución CT-CUM/A-36-2018.

[1] Consultable en: https://www.scjn.gob.mx/sites/default/files/resoluciones/2021-03/CT-CI-A-2-2021.pdf

vMgykxuQVfHoZu758SYfdSYnVUwO1RjhexlyWwF8VmA=

Para llevar a cabo el análisis correspondiente, se tiene en cuenta que en el esquema de nuestro sistema constitucional, 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 todos.

Sin embargo, como lo ha interpretado el Pleno del Alto Tribunal en diversas ocasiones, el derecho de acceso a la información no puede caracterizarse como uno 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 ello[2].

En atención al dispositivo constitucional antes referido, 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.

Para sustentar la clasificación de reserva que hace la Dirección General de Tecnologías de la Información, transcribe el informe que fue materia de análisis en el cumplimiento CT-CUM/A-36-2018, en el que se manifestó, substancialmente, lo siguiente:

- Proporcionar el tipo de ataques permitiría aumentar los ataques informáticos de manera específica contra las versiones y marca de los equipos de seguridad, así como recepción de otros ataques no recibidos o identificados previamente.
- Proporcionar el lugar (lugar de procedencia) permitiría que se aumente el número de ataques desde regiones o zonas donde se tiene permitido el flujo de tráfico hacia los portales de internet de este Alto Tribunal.

Los argumentos expuestos en la resolución CT-CUM/A-36-2018, permiten confirmar que la información requerida se clasifica como **reservada**, con apoyo en el artículo 113, fracción I, de la Ley General de Transparencia, en virtud de que se podrían poner en riesgo cuestiones de seguridad pública, pues si se divulgara la información solicitada, posibilitaría el aumento de los ataques informáticos, de manera específica contra las versiones y marca de los equipos de seguridad desde regiones o zonas donde se tiene permitido el flujo de tráfico hacia los portales de internet de este Alto Tribunal.

En ese tenor, debe destacarse que el informe lo emite el área técnica que, conforme a sus atribuciones, es responsable del manejo de los equipos a través de los cuales se gestiona la información, por lo que considerando lo resuelto por este Comité en el expediente CTCUM/A-36-2018, se arriba a la conclusión que sobre la información requerida sí pesa la reserva

[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. 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)*'

vMgykxuQVfHoZu758SYfdSYnVUwO1RjhexlyWwF8VmA=

establecida en la fracción I, del artículo 113, de la Ley General de Transparencia que establece:

> '***Artículo 113***. *Como información reservada podrá clasificarse aquella cuya publicación:*
> *I. Comprometa la seguridad nacional, la seguridad pública o la defensa nacional y cuente con un propósito genuino y un efecto demostrable;'*
> (…)

En efecto, acorde con lo resuelto por este Comité en la resolución CT-CUM/A-36-2018, *'desde una óptica general, el objeto de la restricción de la información, como se ha visto, comprende garantizar el buen funcionamiento de los sistemas de seguridad informáticos ante posibles ataques cibernéticos*[3] *, que en general pondrían en riesgo la información de este Alto Tribunal (tanto del quehacer jurisdiccional como administrativo), y con ello daría lugar su posible extracción, modificación o alteración, lo que en última instancia comprometería el ejercicio de los derechos de las personas (acceso a la justicia), lo que es concordante con lo establecido en el artículo décimo octavo, párrafo primero, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de las versiones públicas emitidos por el Sistema Nacional de Transparencia*[4]*'.*

Aunado a lo anterior, se precisó que *'que resulta imperante que se cuenten con sistemas de seguridad basados, entre otros elementos, en una gestión que considere la prevención, detección y respuesta inmediata a los incidentes que afecten a los sistemas en general, tal y como lo disponen los principios 7 y 8 de las Directrices para la seguridad de sistemas y redes de información: hacia una cultura de seguridad*[5] *(directrices), de la OCDE (por sus siglas en inglés: Organisation for Economic Cooperation and Development)'*.

vMgykxuQVfHoZu758SYfdSYnVUwO1RjhexlyWwF8VmA=

---

[3] *'Según el Instituto Nacional de Estándares y Tecnologías (NIST, por sus siglas en inglés), ataque cibernético o 'ciberataque', podría comprender 'un intento de obtener acceso no autorizado a servicios, recursos o información, o un intento de comprometer la integridad, disponibilidad o confidencialidad del sistema' (visible en la siguiente página: https://csrc.nist.gov/Glossary/?term=3015#AlphaIndexDiv). Inclusive se encuentra tipificado como delito por el artículo 211 bis 2, del Código Penal Federal.'*

[4] *'Décimo octavo. De conformidad con el artículo 113, fracción I de la Ley General, podrá considerarse como información reservada, aquella que comprometa la seguridad pública, al poner en peligro las funciones a cargo de la Federación, la Ciudad de México, los Estados y los Municipios, tendientes a preservar y resguardar la vida, la salud, la integridad y el ejercicio de los derechos de las personas, así como para el mantenimiento del orden público…'*

[5] *'**7) Diseño y realización de la seguridad. Los participantes deben incorporar la seguridad como un elemento esencial de los sistemas y redes de información**.*
Los sistemas, las redes y las políticas deberán ser diseñados, ejecutados y coordinados de manera apropiada para optimizar la seguridad. Un enfoque mayor pero no exclusivo de este esfuerzo ha de encontrarse en el diseño y adopción de mecanismos y soluciones que salvaguarden o limiten el daño potencial de amenazas o vulnerabilidades identificadas. Tanto las salvaguardas técnicas como las no técnicas así como las soluciones a adoptar se hacen imprescindibles, debiendo ser proporcionales al valor de la información de los sistemas y redes de información. La seguridad ha de ser un elemento fundamental de todos los productos, servicios, sistemas y redes; y una parte integral del diseño y arquitectura de los sistemas. Para los usuarios finales el diseño e implementación de la seguridad radica fundamentalmente en la selección y configuración de los productos y servicios de sus sistemas.
***8) Gestión de la Seguridad**.*
Los participantes deben adoptar una visión integral de la administración de la seguridad. La gestión de la seguridad debe estar basada en la evaluación del riesgo y ser dinámica, debiendo comprender todos los niveles de las actividades de los participantes y todos los aspectos de sus operaciones. Asimismo ha de incluir posibles respuestas anticipadas a riesgos emergentes y considerar la prevención, detección y respuesta a incidentes que afecten a la seguridad, recuperación de sistemas, mantenimiento permanente, revisión y auditoría. Las políticas de seguridad de los sistemas y redes de información, así como las prácticas, medidas y procedimientos deben estar coordinadas e integradas para crear un sistema coherente de seguridad. Las exigencias en materia de gestión de seguridad dependerán de los niveles de participación, del papel que desempeñan los participantes, del riesgo de que se trate y de los requerimientos del sistema…'

En ese sentido, se tiene presente que en términos del artículo 100, último párrafo, de la Ley General de Transparencia[6], en relación con el 17, párrafo primero, del Acuerdo General de Administración 5/2015[7], es competencia del titular de la instancia que tiene bajo resguardo la información requerida, determinar su disponibilidad y clasificarla conforme a los criterios establecidos en la normativa aplicable.

Así, conforme a lo anterior, la Dirección General de Tecnologías de la Información es el área técnica que cuenta con el personal especializado para velar por la seguridad de la información y de los sistemas tecnológicos del Alto Tribunal, en términos de lo establecido en el artículo 27, fracción I, del Reglamento Orgánico en Materia Administrativa de la Suprema Corte de Justicia de la Nación[8].

En ese sentido, tratándose de cuestiones que atañen a la protección específica de los rubros que involucran aspectos vinculados con la seguridad de los sistemas tecnológicos del Alto Tribunal, es claro que cuando el área enteramente responsable ubica el surgimiento de elementos que inciden en la dimensión ya señalada, el órgano encargado de conocer del acceso sólo debe limitarse a entender y valorar la razonabilidad de la clasificación expresada para efecto de su confirmación o no.

De manera similar a lo argumentado en la resolución CT-CUM/A36-2018, este Comité de Transparencia identifica que se pretende proteger, desde un esquema global, la infraestructura de seguridad informática de este Alto Tribunal, en tanto que se podrían involucrar negativamente aspectos de seguridad pública, y con ello facilitar un ataque cibernético, con repercusiones como son, por una parte, facilitar la extracción, modificación o alteración de información sensible de los expedientes jurisdiccionales, lo que incide directamente en su tarea sustantiva y, por otra parte, *'comprometerse la información administrativa, que generaría un probable riesgo a las personas en lo particular como son trabajadores y proveedores, al hacerse patente un acceso no autorizado ni controlado a los datos personales que se tengan registrados, inclusive, a información contable o bancaria, por solo citar algunos casos.'*

De conformidad con los argumentos señalados, este Comité de Transparencia **confirma la clasificación reservada** de la información relativa al tipo de ataque cibernético y lugar de origen (país de procedencia), con fundamento en el artículo 113, fracción I, de la Ley General de Transparencia.

Con base en lo hasta aquí dicho, este Comité estima que la clasificación antes advertida también se sustenta, desde la especificidad que en aplicación de la prueba de daño mandatan los artículos 103 y 104 de la Ley General, cuya delimitación, como se verá enseguida, necesariamente debe responder a la propia dimensión del supuesto de reserva con el que se relacione su valoración.

---

[6] *'**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.'

[7] *'**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…'

[8] *'**Articulo 27.** El Director General de Tecnologías de la Información tendrá las siguientes atribuciones:*
I. Administrar los recursos en materia de tecnologías de la información y comunicación y proveer los servicios que se requieran en la materia;'
(…)

vMgykxuQVfHoZu758SYfdSYnVUwO1RjhexlyWwF8VmA=

Lo anterior, porque se podrían poner en riesgo cuestiones de seguridad pública, pues según se señaló previamente, a partir de los datos solicitados, si se divulgaran, sería posible perfeccionar un ataque cibernético, o bien intentos de otros no recibidos o identificados hasta el momento, al contar con factores de reconocimiento sobre la infraestructura de seguridad informática de la Suprema Corte de Justicia de la Nación, a partir de los ataques registrados y mitigados, lo que evidentemente si pesa sobre la capacidad de respuesta.

En ese orden de ideas, lo que se impone es **clasificar** como reservada la información a que se hace referencia en este apartado, con fundamento en la fracción I, del artículo 113, de la Ley General de Transparencia, por un plazo de cinco años, atendiendo a lo establecido en el artículo 101[9] de la Ley General de Transparencia.

Por lo expuesto y fundado; se,

R E S U E L V E:

[…]

SEGUNDO. Se confirma la clasificación de reservada, de la información a que se hace referencia en el apartado II del segundo considerando de esta resolución.

[…]”

TERCERO. Requerimiento para actualizar el índice de información reservada. Mediante oficio **DGAJ/CT-80-2026** de veintidós de enero de dos mil veintiséis, la personal titular de la Dirección General de Asuntos Jurídicos y Presidenta del Comité de Transparencia, solicitó a la persona titular de la Unidad de Administración de la Suprema Corte de Justicia de la Nación que girara sus instrucciones a la Dirección General Tecnologías de la Información (en lo sucesivo **DGTI**), con la finalidad de que emitiera un informe sobre la vigencia del plazo de clasificación de la información reservada a que se refirió

[9] *‘**Artículo 101.** Los Documentos clasificados como reservados serán públicos cuando:*
I. Se extingan las causas que dieron origen a su clasificación;
II. Expire el plazo de su clasificación;
III. Exista resolución de una autoridad competente que determine que existe una causa de interés público que prevalece sobre la reserva de la información, o
IV. El Comité de Transparencia considere pertinente la desclasificación, de conformidad con lo señalado en el presente Titulo.
La información clasificada como reservada, según el artículo 113 de esta Ley, podrá permanecer con tal carácter hasta por un periodo de cinco años. El periodo de reserva correrá a partir de la fecha en que se clasifica el documento.
Excepcionalmente, los sujetos obligados, con la aprobación de su Comité de Transparencia, podrán ampliar el periodo de reserva hasta por un plazo de cinco años adicionales, siempre y cuando justifiquen que subsisten las causas que dieron origen a su clasificación, mediante la aplicación de una prueba de daño.
Para los casos previstos por la fracción II, cuando se trate de información cuya publicación pueda ocasionar la destrucción o inhabilitación de la infraestructura de carácter estratégico para la provisión de bienes o servicios públicos, o bien se refiera a las circunstancias expuestas en la fracción IV del artículo 113 de esta Ley y que a juicio de un sujeto obligado sea necesario ampliar nuevamente el periodo de reserva de la información; el Comité de Transparencia respectivo deberá hacer la solicitud correspondiente al organismo garante competente, debidamente fundada y motivada, aplicando la prueba de daño y señalando el plazo de reserva, por lo menos con tres meses de anticipación al vencimiento del periodo.’

vMgykxuQVfHoZu758SYfdSYnVUwO1RjhexlyWwF8VmA=

la resolución de este Comité de Transparencia identificada como **CT-CI/A-2-2021** en el que precisara si el plazo de reserva era susceptible de ampliarse, o bien, si procedía su desclasificación (en tanto que habría transcurrido el plazo de clasificación).

CUARTO. Informe de la DGTI. Por oficio **UASCJN/DGTI/SGPNA/DA-24-2026** de veintiséis de enero de dos mil veintiséis, el Enlace de Transparencia de esa Dirección General remitió la Nota **UASCJN/DGTI/SGSICS-I-1-2026** por la que el Subdirector General de Seguridad Informática y Calidad de Sistemas adscrito a la DGTI dio contestación al requerimiento que antecede, e informó que aún persisten razones para mantener la clasificación de la información como reservada, en los siguientes términos:

"[…]

Al respecto se informa que subsisten las causas que dieron origen a la clasificación de la información como reservada, con fundamento en el artículo 110, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública y la fracción I del artículo 113, de la Ley General de Transparencia y Acceso a la Información Pública, como a continuación se expone:

Conforme al artículo 111 de la Ley Federal de Transparencia y Acceso a la Información Pública los sujetos obligados deben fundar y motivar las causales de reserva previstas en el artículo 110 de dicho ordenamiento, a través de la aplicación de la prueba de daño a la que se refiere el artículo 104. Por su parte, el mencionado artículo 104 establece que, en la justificación de la prueba de daño, el sujeto obligado deberá corroborar lo siguiente:

a) Que la divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público.
b) Que el riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda.
c) Que la limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio.

Por otra parte, el Trigésimo Tercero de los Lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas (Lineamientos Generales), establece que:

'Para la aplicación de la prueba de daño a la que hace referencia el artículo 104 de la Ley General de Transparencia y Acceso a la Información Pública, los sujetos obligados atenderán lo siguiente:

I *Se debe citar la fracción y, en su caso, la causal aplicable del artículo 113 de la Ley General de Transparencia y Acceso a la Información Pública, vinculándola con el Lineamiento específico y, cuando corresponda, el*

vMgykxuQVfHoZu758SYfdSYnVUwO1RjhexlyWwF8VmA=

supuesto normativo que expresamente le otorga el carácter de información reservada.

II *Mediante la ponderación de los intereses en conflicto, los sujetos obligados deben demostrar que la publicidad de la información solicitada generaría un riesgo de perjuicio y por lo tanto, tendrán que acreditar que este último rebasa el interés público protegido por la reserva.*

III *Se debe de acreditar el vínculo entre la difusión de la información y la afectación del interés jurídico tutelado de que se trate.*

IV *Precisar las razones objetivas por las que la apertura de la información generaría una afectación, a través de los elementos de un riesgo real, demostrable e identificable.*

V *En la motivación de la clasificación, el sujeto obligado deberá acreditar las circunstancias de modo, tiempo y lugar del daño.*

VI *Deberán elegir la opción de excepción al acceso a la información que menos lo restrinja, la cual será adecuada y proporcional para la protección del interés público, y deberá interferir lo menos posible en el ejercicio efectivo del derecho de acceso a la información.'*

Bajo este contexto, debe señalarse que la normativa establece las causales de reserva y establece como mecanismo para fundar y motivar tales causales, la aplicación de una prueba de daño que deben proporcionar los sujetos obligados para acreditarse el cumplimiento de elementos que se señalan en el Trigésimo Tercero de los Lineamientos Generales.

Por su parte, el penúltimo párrafo del artículo 99 de la Ley Federal de Transparencia y Acceso a la Información Pública prevé la posibilidad para los sujetos obligados de ampliar el plazo de reserva siempre y cuando justifiquen que subsisten las causas que dieron origen a su clasificación, mediante la aplicación de una prueba de daño.

Por lo anterior, y a fin de fundar y motivar la ampliación del periodo de reserva de la información, se informa que subsisten las causas que dieron origen a la clasificación de la información, por lo que se aplica la siguiente prueba de daño:

- Existe un riesgo real, demostrable e identificable de perjuicio significativo al interés público, en tanto que colocaría a la Suprema Corte de Justicia de la Nación en un estado de vulnerabilidad, facilitando una posible intervención de las comunicaciones; usurpación de permisos; suplantación de equipos y de la información almacenada en los servidores; robo de información que obran en los archivos digitales, así como el detrimento de las instalaciones tecnológicas.

- Se supera el interés público general de que se difunda la información, ya que el resguardo de los datos requeridos 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, copias, modificar, destruir o provocar la pérdida de información contenida en sistemas o equipos de informática, por lo que revelar las políticas de vulnerabilidad implementadas para la prevención y solución de amenazas conforme a cada elemento para la protección de los sistemas de la Suprema Corte de Justicia de la Nación "no sólo se

vMgykxuQVfHoZu758SYfdSYnVUwO1RjhexlyWwF8VmA=

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.

- El proteger la información clasificada como reservada se adecúa al principio de proporcionalidad, 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 la información solicitada, posibilitaría el aumento de los ataques informáticos, de manera específica contra las versiones y marca de los equipos de seguridad desde regiones o zonas donde se tiene permitido el flujo de tráfico hacia los portales de internet de este Alto Tribunal.

- Derivado de todo lo anterior, cabe precisar que el Código Penal Federal 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 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.

vMgykxuQVfHoZu758SYfdSYnVUwO1RjhexlyWwF8VmA=

> 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, 'desde una óptica general, el objeto de la restricción de la información, como se ha visto, comprende garantizar el buen funcionamiento de los sistemas de seguridad informáticos ante posibles ataques cibernéticos, que en general pondrían en riesgo la información de este Alto Tribunal (tanto del quehacer jurisdiccional como administrativo), y con ello daría lugar su posible extracción, modificación o alteración, lo que en última instancia comprometería el ejercicio de los derechos de las personas (acceso a la justicia), y que es concordante con lo establecido en el artículo décimo octavo, párrafo primero, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de las versiones públicas emitidos por el Sistema Nacional de Transparencia'.

En conclusión, es procedente ampliar la reserva de la información, ya que subsisten las causas que dieron origen a su clasificación, con fundamento en los artículos 99, tercer párrafo y 110, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública y la fracción I del artículo 113 de la Ley General de Transparencia y Acceso a la Información Pública.

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, 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. Ese mismo artículo señala que los sujetos obligados, con la aprobación de su Comité de Transparencia, podrán ampliar el periodo de reserva hasta por un plazo de cinco años adicionales, siempre y cuando justifiquen que subsisten las causas que dieron origen a su clasificación, mediante la aplicación de una prueba de daño.

Atendiendo a los argumentos vertidos en la prueba de daño referida, se informa que **al subsistir las causas que dieron origen a la clasificación de información como reservada**, se solicita al Comité de Transparencia **la ampliación del periodo de reserva de la información** de referencia por un periodo de **5 años adicionales**, de conformidad con el artículo 99, tercer párrafo de la Ley Federal de Transparencia y Acceso a la Información Pública.

[…]"

QUINTO. Acuerdo de turno. Por proveído de veintisiete de enero de dos mil veintiséis, la Presidenta del Comité de Transparencia con fundamento

vMgykxuQVfHoZu758SYfdSYnVUwO1RjhexlyWwF8VmA=

en los artículos 44, fracción VIII, 101 y 103 de la Ley General de Transparencia y Acceso a la Información Pública publicada en el Diario Oficial de la Federación (DOF) el cuatro de mayo del dos mil quince, así como 27 del Acuerdo General de Administración 5/2015, integró y registró el expediente y ordenó su remisión a la persona titular del Centro de Documentación y Análisis, Archivos y Compilación de Leyes de esta Suprema Corte de Justicia de la Nación, en su carácter de integrante de dicho órgano, para que conforme a sus atribuciones procediera al estudio y propuesta de la resolución respectiva, lo cual se realizó mediante oficio **CT-30-2026** de esa misma fecha.

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

PRIMERO. Consideración Previa.

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 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", en cuyo artículo Segundo Transitorio[10], en específico en sus fracciones II y III, se establece expresamente la abrogación de la Ley General de Transparencia y Acceso a la Información Pública, publicada en el DOF el cuatro de mayo de dos mil quince y de la Ley Federal de Transparencia y Acceso a la Información Pública, publicada en el mismo medio de difusión el nueve de mayo de dos mil dieciséis (ambas vigentes al momento de la presentación de la solicitud que da origen a la presente resolución).

vMgykxuQVfHoZu758SYfdSYnVUwO1RjhexlyWwF8VmA=

[10] "**Transitorios.**
[…]
Segundo.- A la entrada en vigor del presente Decreto se abrogan las disposiciones siguientes:
[…]
II. La Ley General de Transparencia y Acceso a la Información Pública, publicada en el Diario Oficial de la Federación el 4 de mayo de 2015 y sus modificaciones posteriores.

III. La Ley Federal de Transparencia y Acceso a la Información Pública, publicada en el Diario Oficial de la Federación el 9 de mayo de 2016 y sus modificaciones posteriores;
[…]"

No obstante lo anterior, los artículos Noveno y Décimo[11] transitorios del propio Decreto disponen que **todos aquellos procedimientos iniciados con anterioridad a su entrada en vigor** ante el Instituto Nacional de Transparencia y Protección de Datos Personales (INAI), en materias de transparencia y acceso a la información y de protección de datos personales, **se sustanciarán** 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**.

Por lo tanto, es de concluirse que la legislación abrogada a través del decreto de veinte de marzo de dos mil veinticinco, resulta legal y formalmente aplicable a la solicitud de acceso a la información materia de la presente resolución en todas sus etapas, reglas, plazos, competencias y recursos, incluyendo la competencia de este órgano colegiado, toda vez que, como se puede advertir de los antecedentes descritos, la solicitud con folio **0330000000221** fue presentada en la Plataforma Nacional de Transparencia el **cuatro de enero de dos mil veintiuno,** fecha en la que aún se encontraban vigentes la Ley General de Transparencia y Acceso a la Información Pública (DOF, cuatro de mayo de dos mil quince), y la Ley Federal de Transparencia y Acceso a la Información Pública (DOF, nueve de mayo de dos mil dieciséis), por lo que de conformidad con los referidos preceptos transitorios del Decreto publicado el veinte de marzo de dos mil veinticinco, y en congruencia con los principios de seguridad jurídica y certeza normativa, el análisis y determinación que adopte este Comité de Transparencia se realizarán conforme a la legislación que se encontraba vigente.

vMgykxuQVfHoZu758SYfdSYnVUwO1RjhexlyWwF8VmA=

[11] "**Transitorios**
[…]
Noveno.- Los procedimientos iniciados con anterioridad a la entrada en vigor de este Decreto ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, en materia de acceso a la información pública, se sustanciarán ante Transparencia para el Pueblo conforme a las disposiciones aplicables vigentes al momento de su inicio.
[…]
Décimo.- Los procedimientos iniciados con anterioridad a la entrada en vigor de este Decreto ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, en materia de datos personales o cualquier otra distinta a la mencionada en el transitorio anterior, se sustanciarán conforme a las disposiciones vigentes al momento de su inicio ante la Secretaría Anticorrupción y Buen Gobierno a que se refiere este Decreto.
[…]"

En consecuencia, todas las referencias contenidas en esta resolución a la Ley General de Transparencia y Acceso a la Información Pública (Ley General de Transparencia) y a la Ley Federal de Transparencia y Acceso a la Información Pública (Ley Federal de Transparencia), deberán entenderse hechas a aquellas que se encontraban vigentes al momento de la presentación de la solicitud de acceso la información (cuatro de enero de dos mil veintiuno), conservando de esta manera la validez, competencia y efectos jurídicos para este procedimiento.

SEGUNDO Competencia. Este Comité de Transparencia de la Suprema Corte de Justicia de la Nación es competente para pronunciarse sobre la ampliación del periodo de reserva de la información, en términos de los artículos 6o, apartado A, fracción I, de la Constitución Política de los Estados Unidos Mexicanos, 4, párrafo segundo, 43, 44, fracciones II y VIII, y 101 de la Ley General de Transparencia, así como 23, fracciones I y II, del Acuerdo General de Administración 5/2015.

TERCERO. Análisis sobre la vigencia del plazo de reserva. Al respecto es menester señalar que, de conformidad con los artículos 100, párrafo tercero, de la Ley General de Transparencia[12] y 97, párrafo tercero, de la Ley Federal de Transparencia[13], en correlación con el diverso 17 del Acuerdo General de Administración 05/2015[14], son las personas titulares de las áreas que tienen bajo resguardo la información solicitada, quienes tienen la responsabilidad de determinar su disponibilidad y clasificarla conforme a la normativa aplicable.

Bajo ese tenor, mediante oficio **UASCJN/DGTI/SGPNA/DA-24-2026**, y **Nota UASCJN/DGTI/SGSICS-I-1-2026**, ambos de veintiséis de enero del

[12] "**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."
[13] "**Artículo 97**
[…]
Los titulares de las Áreas de los sujetos obligados serán los responsables de clasificar la información, de conformidad con lo dispuesto en la Ley General y la presente Ley."
[14] "**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.
[…]"

vMgykxuQVfHoZu758SYfdSYnVUwO1RjhexlyWwF8VmA=

presente año, la **DGTI**, en respuesta al oficio **DGAJ/CT-80-2026,** citado en el apartado de antecedentes de esta resolución, indicó esencialmente que, con fundamento en los artículos 113, fracción I, de la Ley General de Transparencia[15] y 110, fracción I, de la Ley Federal de Transparencia[16], **aún persisten las causas para clasificar como reservada cierta información relativa** a los ataques cibernéticos que registró la institución, del primero de enero de dos mil veinte al cuatro de enero de dos mil veintiuno, **en específico lo concerniente al tipo de ataque y país de procedencia**, cuya clasificación fue confirmada por este órgano colegiado al resolver el expediente **CT-CI/A-2-2021** el veintisiete de enero de dos mil veintiuno.

Para justificar la ampliación de la reserva de la información, en acatamiento a lo dispuesto por los artículos 104 de la Ley General de Transparencia y 111 de la Ley Federal de Transparencia, la instancia que tiene bajo resguardo la información realizó la aplicación de una prueba de daño, misma que se funda y motiva en las siguientes consideraciones:

Elemento que debe justificarse	Justificación
La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público o a la seguridad nacional	- La divulgación de la información facilitaría una posible intervención, usurpación, suplantación o robo de las comunicaciones, permisos, así como la extracción, modificación o alteración de la información contenida en las instalaciones tecnológicas de esta Suprema Corte de Justicia de la Nación, lo que la colocaría en un estado de vulnerabilidad.

[15] "**Artículo 113.** Como información reservada podrá clasificarse aquella cuya publicación:
I. Comprometa la seguridad nacional, la seguridad pública o la defensa nacional y cuente con un propósito genuino y un efecto demostrable;
[…]".
[16] "**Articulo 110**. Conforme a lo dispuesto por el artículo 113 de la Ley General, como información reservada podrá clasificarse aquella cuya divulgación:
I. Comprometa la seguridad nacional, la seguridad pública o la defensa nacional y cuente con un propósito genuino y un efecto demostrable;
[…]".

vMgykxuQVfHoZu758SYfdSYnVUwO1RjhexlyWwF8VmA=

El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda	- Se supera el interés público de que se difunda la información, toda vez la reserva de la información se justifica en llevar a cabo la prevención del delito de “Acceso ilícito y equipos de informática”, tipificado en el Código Penal Federal, evitando revelar políticas implementadas por esta Institución para la protección de sus sistemas, que, de revelarse, proporcionarían información que podría permitir que se ejecuten ataques informáticos a la infraestructura tecnológica de este Alto Tribunal. - La divulgación no solo comprometería la información de los archivos digitales de esta Suprema Corte, si no que podría vulnerar la seguridad y certeza de aquellos que acuden ante esta Institución.
La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio	- La reserva se adecua al principio de proporcionalidad y representa el medio menos restrictivo para evitar el perjuicio, en virtud de que su difusión daría a conocer de manera específica las versiones, marca de los equipos de seguridad, regiones y zonas donde se tiene permitido el flujo de tráfico de internet en esta Suprema Corte, lo que posibilitaría el aumento de los ataques informáticos.

vMgykxuQVfHoZu758SYfdSYnVUwO1RjhexlyWwF8VmA=

Además, la **DGTI** mencionó que el objeto de la restricción de la información encuentra su cause en garantizar el buen funcionamiento de los sistemas de seguridad informáticos con los que cuenta esta Suprema Corte de Justicia de la Nación ante posibles ataques cibernéticos, por lo que solicita la ampliación del periodo de reserva por un periodo de **cinco años.**

A partir de lo señalado por la **DGTI**, este Comité de Transparencia considera que se encuentra justificada la ampliación del plazo de reserva, porque del análisis de la prueba de daño aplicada por el área vinculada, se desprende que:

- La divulgación del tipo de ataque y el país de procedencia de los ataques cibernéticos registrados entre el primero de enero del año dos mil veinte al siete de enero del año dos mil veintiuno habilitaría la posibilidad de que esta información facilitará una posible intervención, usurpación, suplantación o robo de las comunicaciones, permisos, así como la extracción, modificación o alteración de la información contenida en las instalaciones tecnológicas de esta Suprema Corte de Justicia de la Nación, toda vez que estos datos por sí solos o en conjunto con el número de ataques registrados, que fueron entregados en la clasificación originaria, tienen el potencial de revelar la capacidad de soporte de la infraestructura tecnológica de seguridad informática, por lo cual se colocaría a este Tribunal Constitucional en un estado de vulnerabilidad en la medida de que estos datos pueden ser utilizados para propiciar el aumento y especificidad de ataques cibernéticos, o bien, el perfeccionamiento de aquellos que se han recibido hasta el momento.
- Además, no solo se comprometen aquellos archivos administrativos que contienen información personal y sensible de trabajadores y proveedores, si no también aquella que es proporcionada por aquellas personas que acuden ante esta Institución con el ánimo de que ejerza su función jurisdiccional, vulnerando los principios constitucionales de seguridad y certeza en los procedimientos.

A mayor abundamiento, se retoma lo sustentado por este Comité de Transparencia al resolver el expediente **CT-CUM/A-52-2023**[17], en el sentido de que el daño que se podría producir con la divulgación de la información relativa al tipo y lugar de origen de los ataques cibernéticos recibidos por la Suprema Corte de Justicia de la Nación *"podría poner en riesgo la infraestructura de los portales electrónicos; asimismo, se facilitaría la extracción, modificación o alteración de información relevante, lo que incidiría directa y negativamente en la tarea sustantiva de este Alto Tribunal y, por otra parte, se podría comprometer la información administrativa"*, así como el

[17] Disponible en: https://www.scjn.gob.mx/sites/default/files/resoluciones/2023-11/CT-CUM-A-52-2023.pdf

vMgykxuQVfHoZu758SYfdSYnVUwO1RjhexlyWwF8VmA=

expediente **CT-CUM-R/A-2-2019**[18], en el cual se expuso que *"La divulgación de la información solicitada 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 una posible intervención de las comunicaciones; usurpación de permisos; suplantación de equipos y de la información almacenada en los servidores; robo de información que obran en los archivos digitales, así como el detrimento de las instalaciones tecnológicas."*.

Bajo ese tenor, la reserva de los datos de referencia representa el medio menos restrictivo del derecho de acceso a la información, al considerarse la trascendencia de proteger, desde un esquema global, la infraestructura de seguridad informática de este Alto Tribunal, en tanto que se podrían involucrar negativamente aspectos de seguridad pública, y con ello facilitar un ataque cibernético.

No pasa desapercibido para este órgano colegiado que la **DGTI**, en su informe, justificó, en cierta medida, la ampliación del plazo de reserva bajo la idea de la prevención de un delito del orden federal, como lo es el acceso ilícito a sistemas y equipo de informática. Al respecto, resulta pertinente señalar que las leyes aplicables en la materia prevén, dentro de su catálogo de causales de reserva la divulgación cuando se obstruya la prevención o persecución de los delitos (fracción VII, del artículo 113, de la Ley General de Transparencia, y 110, de la Ley Federal de Transparencia).

No obstante, el presente caso se circunscribe al análisis de la ampliación del plazo de clasificación en los términos en los que esta fue planteada, es decir, con fundamento en la fracción I del numeral 113 de la Ley General de Transparencia (misma fracción del artículo 110 de la Ley Federal de Transparencia, dada la similitud de contenido).

Ciertamente, en la resolución CT-CI/A-2-2021 se argumentó lo siguiente:

[18] Disponible en: https://www.scjn.gob.mx/sites/default/files/resoluciones/2019-03/CT-CUM-R-A-2-2019.pdf

vMgykxuQVfHoZu758SYfdSYnVUwO1RjhexlyWwF8VmA=

"[…]

Para sustentar la clasificación de reserva que hace la Dirección General de Tecnologías de la Información, transcribe el informe que fue materia de análisis en el cumplimiento CT-CUM/A-36-2018, en el que se manifestó, substancialmente, lo siguiente:

- Proporcionar el tipo de ataques permitiría aumentar los ataques informáticos de manera específica contra las versiones y marca de los equipos de seguridad, así como recepción de otros ataques no recibidos o identificados previamente.
- Proporcionar el lugar (lugar de procedencia) permitiría que se aumente el número de ataques desde regiones o zonas donde se tiene permitido el flujo de tráfico hacia los portales de internet de este Alto Tribunal.

Los argumentos expuestos en la resolución CT-CUM/A-36-2018, permiten confirmar que la información requerida se clasifica como **reservada**, con apoyo en el artículo 113, fracción I, de la Ley General de Transparencia, en virtud de que se podrían poner en riesgo cuestiones de seguridad pública, pues si se divulgara la información solicitada, posibilitaría el aumento de los ataques informáticos, de manera específica contra las versiones y marca de los equipos de seguridad desde regiones o zonas donde se tiene permitido el flujo de tráfico hacia los portales de internet de este Alto Tribunal.

En ese tenor, debe destacarse que el informe lo emite el área técnica que, conforme a sus atribuciones, es responsable del manejo de los equipos a través de los cuales se gestiona la información, por lo que considerando lo resuelto por este Comité en el expediente CTCUM/A-36-2018, se arriba a la conclusión que sobre la información requerida sí pesa la reserva establecida en la fracción I, del artículo 113, de la Ley General de Transparencia que establece:

'***Artículo 113***. *Como información reservada podrá clasificarse aquella cuya publicación:*
I. Comprometa la seguridad nacional, la seguridad pública o la defensa nacional y cuente con un propósito genuino y un efecto demostrable;'
(…)

[…]

En ese sentido, tratándose de cuestiones que atañen a la protección específica de los rubros que involucran aspectos vinculados con la seguridad de los sistemas tecnológicos del Alto Tribunal, es claro que cuando el área enteramente responsable ubica el surgimiento de elementos que inciden en la dimensión ya señalada, el órgano encargado de conocer del acceso sólo debe limitarse a entender y valorar la razonabilidad de la clasificación expresada para efecto de su confirmación o no.

De manera similar a lo argumentado en la resolución CT-CUM/A-36-2018, este Comité de Transparencia identifica que se pretende proteger, desde un esquema global, la infraestructura de seguridad informática de este Alto Tribunal, en tanto que se podrían involucrar negativamente aspectos de seguridad pública, y con ello facilitar un ataque cibernético, con

vMgykxuQVfHoZu758SYfdSYnVUwO1RjhexlyWwF8VmA=

repercusiones como son, por una parte, facilitar la extracción, modificación o alteración de información sensible de los expedientes jurisdiccionales, lo que incide directamente en su tarea sustantiva y, por otra parte, *'comprometerse la información administrativa, que generaría un probable riesgo a las personas en lo particular como son trabajadores y proveedores, al hacerse patente un acceso no autorizado ni controlado a los datos personales que se tengan registrados, inclusive, a información contable o bancaria, por solo citar algunos casos.'*

De conformidad con los argumentos señalados, este Comité de Transparencia **confirma la clasificación reservada** de la información relativa al tipo de ataque cibernético y lugar de origen (país de procedencia), con fundamento en el artículo 113, fracción I, de la Ley General de Transparencia.

[…]

En ese orden de ideas, lo que se impone es **clasificar** como reservada la información a que se hace referencia en este apartado, con fundamento en la fracción I, del artículo 113, de la Ley General de Transparencia, por un plazo de cinco años, atendiendo a lo establecido en el artículo 101 de la Ley General de Transparencia.

[…]"

[Subrayado propio]

En consecuencia, acorde con los artículos 44, fracción VIII[19], y 103[20] de la Ley General de Transparencia, **se determina justificado ampliar el periodo de reserva de la información** decretada por este órgano colegiado con dicho carácter en la resolución dictada en el expediente **CT-CI/A-2-2021,** el veintisiete de enero de dos mil veintiuno**,** al actualizarse la hipótesis prevista en la fracción **I**[21]**,** de los artículos 113 de la Ley General de Transparencia y 110 de la Ley Federal de Transparencia, pues la divulgación de dicha información representa un riesgo real, demostrable e identificable.

vMgykxuQVfHoZu758SYfdSYnVUwO1RjhexlyWwF8VmA=

[19] **"Artículo 44.** Cada Comité de Transparencia tendrá las siguientes funciones:
[…]
VIII. Solicitar y autorizar la ampliación del plazo de reserva de la información a que se refiere el artículo 101 de la presente Ley, y
[…]"

[20] **"Artículo 103** En los casos en que se niegue el acceso a la información, por actualizarse alguno de los supuestos de clasificación, el Comité de Transparencia deberá confirmar, modificar o revocar la decisión.

Para motivar la clasificación de la información y la ampliación del plazo de reserva, se deberán señalar las razones, motivos o circunstancias especiales que llevaron al sujeto obligado a concluir que el caso particular se ajusta al supuesto previsto por la norma legal invocada como fundamento. Además, el sujeto obligado deberá, en todo momento, aplicar una prueba de daño.

Tratándose de aquella información que actualice los supuestos de clasificación, deberá señalarse el plazo al que estará sujeto la reserva."

[21] Establecen que la información podrá ser clasificada como reservada cuando su publicación:
I. Comprometa la seguridad nacional, la seguridad pública o la defensa nacional y cuente con un propósito genuino y un efecto demostrable.
V. Pueda poner en riesgo la vida, seguridad o salud de una persona física.

Por lo expuesto, este Comité determina la ampliación del plazo de clasificación de los datos que fueron materia de *reserva*, por **cinco años,** que se computarán a partir del vencimiento del primer periodo, de conformidad con lo dispuesto en los artículos 99, párrafo tercero, de la Ley Federal de Transparencia y 101, párrafo tercero de la Ley General de Transparencia; en el entendido de que podrá concluir previamente siempre que se actualice alguno de los supuestos de publicidad previstos en el referido artículo 101 de la misma Ley General.

Por lo expuesto y fundado, se

R E S U E L V E:

ÚNICO. Se autoriza la ampliación del plazo de reserva de la información materia de análisis de la presente resolución.

Notifíquese a la instancia vinculada, así como a la Unidad de Transparencia y, en su oportunidad, archívese como asunto concluido.

Así, por unanimidad de votos, lo resolvió el Comité de Transparencia de la Suprema Corte de Justicia de la Nación y firman la **Maestra Camelia Gaspar Martínez**, Directora General de Asuntos Jurídicos y Presidenta del Comité; el **Maestro Abraham Montes Magaña**, Titular de la Unidad de Transparencia de la Suprema Corte de Justicia de la Nación, y el **Doctor Gustavo Miguel Meixueiro Nájera**, Director General del Centro de Documentación y Análisis, Archivos y Compilación de Leyes; integrantes del Comité, ante la Secretaria del Comité, quien autoriza y da fe.

MAESTRA CAMELIA GASPAR MARTÍNEZ
PRESIDENTA DEL COMITÉ

vMgykxuQVfHoZu758SYfdSYnVUwO1RjhexlyWwF8VmA=

MAESTRO ABRAHAM MONTES MAGAÑA
INTEGRANTE DEL COMITÉ

DOCTOR GUSTAVO MIGUEL MEIXUEIRO NÁJERA
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.”

vMgykxuQVfHoZu758SYfdSYnVUwO1RjhexlyWwF8VmA=