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

CUMPLIMIENTO CT-CUM/A-9-2025
Derivado del expediente CT-CI/A-7-2020

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 veintiuno de mayo de dos mil veinticinco.

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

PRIMERO. Solicitud de información. El catorce de mayo de dos mil veinte, se recibió la solicitud tramitada en la Plataforma Nacional de Transparencia con el folio 0330000152820, requiriendo:

> *"1. ¿Qué funciones tienen sus sistemas informáticos en el desarrollo de datos y procesamiento de los mismos?*
> *2. ¿Qué elementos contemplan en la protección de sus sistemas sistemas* (sic) *(amenazas y vulnerabilidades)?*
> *3. Sus políticas de seguridad implementadas para la prevención y solución de amenazas conforme a cada elemento para la protección de los sistemas.*
> *4. Cuerpos normativos y artículos a los que se vincula la seguridad informática de los sistemas de cómputo y/o bases de datos."*

SEGUNDO. Resolución del Comité de Transparencia en la que se clasificó información. En sesión de diecisiete de junio de dos mil veinte, este Comité de Transparencia emitió resolución en el expediente CT-CI/A-7-2020[1], conforme se transcribe en lo conducente:

> *"**SEGUNDO. Análisis.** En la solicitud se pide información de la Suprema Corte de Justicia de la Nación, consistente en:*
>
> 1. *Tipo de funciones que se utilizan en los sistemas informáticos en el desarrollo y procesamiento de datos.*

[1] Disponible en: https://www.supremacorte.gob.mx/sites/default/files/resoluciones/2020-08/CT-CI-A-7-2020.pdf

nosXVDDVmmAajYnub+SVojgz3by7vwgi5YYS9wAmkOM=

2. *Elementos que se contemplan en la protección de los sistemas sobre amenazas y vulnerabilidades.*
3. *Las políticas de vulnerabilidad implementadas para la prevención y solución de amenazas conforme a cada elemento para la protección de los sistemas.*
4. *Normativa que se vincula con la seguridad informática de los sistemas de cómputo y bases de datos.*

(…)

II. Información reservada.

Por cuanto a las políticas de vulnerabilidad implementadas para la prevención y solución de amenazas conforme a cada elemento para la protección de los sistemas que se requiere en el punto 3 de la solicitud, la Dirección General de Tecnologías de la Información clasifica dicha información como reservada, aduciendo que con su acceso se ponen en riesgo los sistemas de datos de este Alto Tribunal que no son públicos, ya que se daría a conocer información técnica sobre los equipos de cómputo, los protocolos de seguridad y las características de la infraestructura instalada.

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.

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 <u>temporalmente reservada o confidencial</u> en los términos establecidos por el legislador federal o local, cuando de su propagación pueda derivarse perjuicio por causa de interés público y seguridad nacional.

Ahora bien, para sustentar la clasificación de reserva que hace la Dirección General de Tecnologías de la Información, se cita el artículo 110, fracción VII, de la Ley Federal de Transparencia, manifestando que su divulgación:

- *Permitiría el acceso ilícito a los sistemas y equipos, ejerciendo la suplantación de estos.*
- *Potenciaría la posibilidad de vulnerar la infraestructura tecnológica.*
- *Establecería con alto grado de precisión la información técnica sobre los protocolos de seguridad y las características de la infraestructura instalada.*

nosXVDDVmmAajYnub+SVojgz3by7vwgi5YYS9wAmkOM=

- *Se pondría en estado vulnerable a la Suprema Corte de Justicia de la Nación, porque se facilitaría la intervención de las comunicaciones, permitiendo usurpar los permisos requeridos en la red para obtener información.*
- *Daría a conocer puntos de vulnerabilidad para la seguridad de la infraestructura de cómputo.*
- *Vulneraría los sistemas informáticos y la información contenida en éstos.*
- *Atentaría contra la infraestructura tecnológica, afectando el ejercicio de las labores sustantivas.*
- *Modificaría, destruiría o provocaría pérdida de información contenida en los sistemas informáticos.*

*La clasificación como **reservada** de dicha información, como se señaló, se sustenta en el artículo 110, fracción VII, de la Ley Federal de Transparencia, en virtud de que al poner en riesgo cuestiones de seguridad y conectividad de los sistemas informáticos y bases de datos de la Suprema Corte de Justicia de la Nación se obstruiría la prevención de delitos, específicamente, delito de acceso ilícito a sus equipos y sistemas de informática.*

En ese tenor, es importante destacar que el informe que se analiza lo emite el área técnica que, conforme a sus atribuciones, es responsable en la Suprema Corte de Justicia de la Nación de los sistemas informáticos de los que se pide la información, por lo que considerando lo resuelto por este Comité en el cumplimiento CT-CUM-R/A-2-2019, se arriba a la conclusión de que sobre la información requerida sí pesa la reserva establecida en la fracción VII del artículo 110, de la Ley Federal de Transparencia que establece:

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

*Sobre el alcance del artículo 110, fracción VII, de la Ley Federal de Transparencia, se tienen en cuenta que su contenido es idéntico al que dispone la Ley General de Transparencia en el artículo 113, fracción VII, razón por la que se tiene presente lo resuelto por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales en el recurso de revisión RRA 10276/18, cumplimentado por este Comité en la citada resolución CT-CUM-R/A-2-2019, ya que se señaló que ‘como información reservada podrá clasificarse aquella cuya publicación obstruya la prevención o persecución de delitos’, agregando que ‘para que pueda acreditarse que la información requerida pudiera ‘obstruir la prevención de los delitos’, debe vincularse a la **afectación a las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de las autoridades para evitar la comisión de delitos**’ (página 98, vuelta de la resolución del recurso de revisión RRA 10276/18).*

Además, en dichas resoluciones se precisa 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, agregando: ‘por definición

nosXVDDVmmAajYnub+SVojgz3by7vwgi5YYS9wAmkOM=

*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' y 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 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).*

Adicionalmente, es de destacar que, en la resolución emitida por el Instituto Nacional de Transparencia se invocan, como hecho notorio, las respuestas que la Dirección General de Tecnologías de la Información de ese Instituto emitió en respuesta a las consultas que se le formularon sobre información similar a la que es materia de la solicitud que da origen a este asunto.

*En virtud de lo anterior, en la resolución del Instituto Nacional de Transparencia 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'.*

*De conformidad con lo expuesto, atendiendo a los argumentos señalados por el Instituto Nacional de Transparencia en el recurso de revisión RRA 10276/18 y que fueron retomados en la resolución CT-CUM-R/A-2-2-2019, este Comité de Transparencia **confirma la clasificación de reserva** de la información relativa a 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 (punto 3 de la solicitud), con fundamento en los artículos 113, fracción VII, de la Ley General de Transparencia y 110, fracción VII, de la Ley Federal de la materia, dado que, como se mencionó, considerando que la Dirección General de Tecnologías de la Información es el área técnica para pronunciarse sobre la naturaleza de la información solicitada y dicha área señaló que al entregar esos datos se podría comprometer la seguridad informática de los sistemas y*

nosXVDDVmmAajYnub+SVojgz3by7vwgi5YYS9wAmkOM=

equipos de este Alto Tribunal, porque se pondría en riesgo la seguridad operativa de la infraestructura tecnológica que permite la operación de las diversas áreas del Alto Tribunal.

Así, conforme a la argumentación sostenida en la resolución del Instituto Nacional de Transparencia la reserva de dicha información permite prevenir la comisión del delito de acceso ilícito a sistemas y equipos de informática tipificados en el Código Penal Federal, pues al dar a conocer la información solicitada, 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'.

Por lo tanto, se confirma se confirma la reserva de la información materia de este apartado, con fundamento en los artículos 110, fracción VII, de la Ley Federal de Transparencia y 113, fracción VII, de la Ley General de Transparencia.

***Análisis específico de la prueba de daño**. De acuerdo con el alcance de la causa de reserva prevista en el artículo 110, fracción VII, de la Ley Federal de Transparencia, acorde con lo señalado por el Instituto Nacional de Transparencia al resolver el recurso de revisión RRA 10276/18 y por este Comité en la resolución de cumplimiento CT-CUM-R/A-2-2019, se determina 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.*

*En ese sentido, el perjuicio significativo al **interés público** resulta **menos restrictivo**, porque se pondría en riesgo la responsabilidad fundamental del Alto Tribunal en la defensa del orden establecido en la Constitución Federal, mediante los medios de control constitucional.*

Por lo anterior, 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 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 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'.

nosXVDDVmmAajYnub+SVojgz3by7vwgi5YYS9wAmkOM=

> *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 las políticas de vulnerabilidad implementadas para la prevención y solución de amenazas de los sistemas informáticos '**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.** En términos de lo señalado en el artículo 101, párrafo segundo, de la Ley General de Transparencia, se determina que el plazo de reserva será por cinco años, ya que por las consideraciones expuestas en la resolución del Instituto Nacional de Transparencia a que se hacho mención y en la de cumplimiento CT-CUM-R/A-2-2019, mismas que se retoman en esta determinación, 'dicho plazo es proporcional a la naturaleza y el grado de especificidad del tipo de información de que se trata'.*
>
> *Por lo expuesto y fundado; se,*
>
> ***R E S U E L V E:***
>
> ***PRIMERO.** Se tiene por atendida la solicitud en términos de lo expuesto en el considerando segundo de la presente resolución.*
>
> ***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.** Se requiere a la Unidad General de Transparencia para que realice las acciones señaladas en esta resolución."*

TERCERO. **Requerimiento para actualizar el índice de información reservada.** Mediante oficio CT-120-2025, enviado por correo electrónico el veintiocho de abril de dos mil veinticinco, la Secretaría de este Comité de Transparencia solicitó a la Dirección General de Tecnologías de la Información (Tecnologías de la Información) que se pronunciara sobre la vigencia de la reserva de la información clasificada en la resolución transcrita o si procedía su desclasificación.

nosXVDDVmmAajYnub+SVojgz3by7vwgi5YYS9wAmkOM=

CUARTO. Informe de Tecnologías de la Información. El catorce de mayo de dos mil veinticinco, se remitió por correo electrónico el oficio DGTI-212-2025[2], con el que, a su vez, se remitió la Atenta Nota con número *"DGTI/SGSICS-I-12-2025"*, de la Subdirección General de Seguridad Informática y Calidad de Sistemas, en la que se señala:

> *"En primera instancia, se aclara que, si bien el 20 de marzo de 2025 se publicó en el Diario Oficial de la Federación el DECRETO por el que se expiden la Ley General de Transparencia y Acceso a la Información Pública; la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; la Ley Federal de Protección de Datos Personales en Posesión de los Particulares; y se reforma el artículo 37, fracción XV, de la Ley Orgánica de la Administración Pública Federal (del que se inserta vínculo electrónico para consulta), que abroga la normativa a la que se hace referencia en el presente nota; el artículo Noveno Transitorio del referido Decreto indica que los procedimientos iniciados con anterioridad a su entrada en vigor, en materia de acceso a la información pública, se sustanciarán conforme a las disposiciones aplicables vigentes al momento de su inicio. En ese sentido, tomando en consideración que la solicitud que dio origen a la clasificación que nos ocupa se recibió el 14 de mayo de 2020, es necesario realizar el análisis con fundamento en las leyes de la materia vigentes al momento en que fue presentada.*
>
> *Ahora bien, el folio antes citado está relacionado con la siguiente información:*
>
> > *'1. ¿Qué funciones tienen sus sistemas informáticos en el desarrollo de datos y procesamiento de los mismos?*
> > *2. ¿Qué elementos contemplan en la protección de sus sistemas sistemas (sic) (amenazas y vulnerabilidades)?*
> > *3. Sus políticas de seguridad implementadas para la prevención y solución de amenazas conforme a cada elemento para la protección de los sistemas.*
> > *4. Cuerpos normativos y artículos a los que se vincula la seguridad informática de los sistemas de cómputo y/o bases de datos.' (sic)*
>
> *Se precisa que la Dirección General de Tecnologías en la atención de esa solicitud de acceso a la información, proporcionó información para dar atención a los puntos 1, 2 y 4.*
>
> *Por lo que hace al punto 3, se clasificó como reservada la información, manifestando que con su acceso se ponen en riesgo los sistemas de datos de este Alto Tribunal que no son públicos, ya que se daría a conocer información técnica sobre los equipos de cómputo, los protocolos de seguridad y las características de la infraestructura instalada.*
>
> *Al respecto se informa que subsisten las causas que dieron origen a la clasificación de la información como reservada, con fundamento en el artículo 113 fracción VII de la ahora abrogada Ley General de Transparencia y Acceso a la Información Pública aún aplicable al caso, como a continuación se expone:*

[2] También se remitió por el Sistema de Gestión Documental Institucional el quince de mayo de dos mil veinticinco.

nosXVDDVmmAajYnub+SVojgz3by7vwgi5YYS9wAmkOM=

Es importante 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.

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 las políticas de seguridad informática podría ocasionar lo siguiente:

- ✓ *Una posible intervención de sus comunicaciones;*
- ✓ *La usurpación de sus permisos;*
- ✓ *La suplantación de sus equipos y de la información que almacena en sus servidores;*
- ✓ *El robo de la información que obra en sus archivos digitales, y*
- ✓ *El detrimento de sus instalaciones tecnológicas.*

nosXVDDVmmAajYnub+SVojgz3by7vwgi5YYS9wAmkOM=

Cuestiones que se materializan con la comisión de delitos de carácter cibernético, que sin duda afectarían severamente el ejercicio de las labores cotidianas y sustantivas de este Alto Tribunal.

Indicado lo anterior, conforme al artículo 111 de la Ley Federal de Transparencia y Acceso a la Información Pública (abrogada que aplicable al presente caso) 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) –aplicables al presente caso–, 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 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.

nosXVDDVmmAajYnub+SVojgz3by7vwgi5YYS9wAmkOM=

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 tal como se ha referido con anterioridad, lo cual cobra importancia si se considera que dicha conducta implica conocer, copiar, modificar, destruir o provocar la pérdida de información contenida en sistemas o equipos de informática, por lo que revelar las 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 comprometería la información que obra en los archivos digitales del sujeto obligado, sino que menoscabaría la seguridad y certeza de las personas que acuden a 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 de las políticas de vulnerabilidad implementadas para la prevención y solución de amenazas de los sistemas informáticos '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.*

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 VII de la ahora abrogada Ley Federal de Transparencia y Acceso a la Información Pública y la fracción VII

nosXVDDVmmAajYnub+SVojgz3by7vwgi5YYS9wAmkOM=

del artículo 113 de la también abrogada Ley General de Transparencia y Acceso a la Información Pública, ambas aún aplicables al presente asunto.

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 abrogada Ley Federal de Transparencia y Acceso a la Información Pública.

Por último, todo lo anteriormente expuesto se refuerza con lo resuelto por el Comité de Transparencia a través del expediente de cumplimiento CT-CI/A-7-2020.”

QUINTO. Acuerdo de turno. Mediante proveído de quince de mayo de dos mil veinticinco, con fundamento 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 el cuatro de mayo del dos mil quince (Ley General de Transparencia), así como 27 del Acuerdo General de Administración 5/2015, la Presidencia del Comité de Transparencia de este Alto Tribunal ordenó integrar el expediente de cumplimiento **CT-CUM/A-9-2025** y remitirlo al Contralor del Alto Tribunal, lo que se hizo mediante oficio CT-143-2025, enviado por correo electrónico en la misma fecha.

nosXVDDVmmAajYnub+SVojgz3by7vwgi5YYS9wAmkOM=

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

PRIMERA. Competencia. Para determinar el fundamento de la competencia de este Comité de Transparencia para conocer y resolver sobre el presente asunto, se recuerda que el veinte de marzo de dos mil veinticinco se publicó en el 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,* cuyo artículo Segundo Transitorio estableció la **abrogación** de diversas leyes, entre ellas, la Ley General de Transparencia publicada en el DOF el cuatro de mayo de dos mil quince y la Federal de Transparencia y Acceso a la Información Pública (Ley Federal de Transparencia) publicada en el DOF el nueve de mayo de dos mil dieciséis.

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

Ahora, se destaca que el procedimiento de acceso a la información pública se compone por diversas etapas, las cuales, genéricamente,

nosXVDDVmmAajYnub+SVojgz3by7vwgi5YYS9wAmkOM=

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

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

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

nosXVDDVmmAajYnub+SVojgz3by7vwgi5YYS9wAmkOM=

A partir de lo expuesto, 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 6° de la Constitución Política de los Estados Unidos Mexicanos, 4 y 44, fracción VIII, y 101, párrafo tercero, de la Ley General de Transparencia, así como 23, fracción I, del Acuerdo General de Administración 5/2015.

SEGUNDA. Análisis. Para efectos de esta resolución de cumplimiento, se precisa que la materia se constriñe a determinar si se amplía o no el plazo de reserva de la información analizada en la resolución CT-CI/A-7-2020, consistente en las políticas de vulnerabilidad implementadas la prevención y solución de amenazas conforme a cada elemento para la protección de los sistemas que se pidió en el punto 3 de la solicitud de origen.

En ese sentido, Tecnologías de la Información señala que subsisten las causas para mantener reservada dicha información, con fundamento en el artículo 113, fracción VII, de la Ley General de Transparencia.

Para realizar el análisis correspondiente, se tiene en cuenta que conforme a los artículos 100[3] de la Ley General de Transparencia y 97[4] de

[3] *"**Artículo 100.** La clasificación es el proceso mediante el cual el sujeto obligado determina que la información en su poder actualiza alguno de los supuestos de reserva o confidencialidad, de conformidad con lo dispuesto en el presente Título.*
Los supuestos de reserva o confidencialidad previstos en las leyes deberán ser acordes con las bases, principios y disposiciones establecidos en esta Ley y, en ningún caso, podrán contravenirla.
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."

[4] "***Artículo 97.** La clasificación es el proceso mediante el cual el sujeto obligado determina que la información en su poder actualiza alguno de los supuestos de reserva o confidencialidad, de conformidad con lo dispuesto en el presente Título.*
En el proceso de clasificación de la información, los sujetos obligados observarán, además de lo establecido en el Título Sexto de la Ley General, las disposiciones de la presente Ley.
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.

nosXVDDVmmAajYnub+SVojgz3by7vwgi5YYS9wAmkOM=

la Ley Federal de Transparencia, en relación con el diverso 17[5] del Acuerdo General de Administración 5/2015, las instancias que tienen bajo resguardo la información solicitada son las responsables de determinar su disponibilidad y clasificarla conforme a la normativa aplicable.

En ese sentido, se destaca que en términos del artículo 36, fracciones I, V, VI y IX[6], del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación, Tecnologías de la Información es el área técnica que cuenta con el personal especializado para velar por la seguridad de los sistemas tecnológicos de este Alto Tribunal, pues le corresponde administrar sus sistemas informáticos administrativos y jurisdiccionales.

Conforme a ello y acorde con los argumentos expuestos en la resolución CT-CI/A-7-2020, se considera que prevalecen las razones que actualizan la hipótesis prevista en el artículo 113, fracción VII[7], de la Ley

---

Los sujetos obligados deberán aplicar, de manera restrictiva y limitada, las excepciones al derecho de acceso a la información previstas en el presente Título y deberán acreditar su procedencia, sin ampliar las excepciones o supuestos de reserva o confidencialidad previstos en las leyes, de conformidad con lo establecido en la Ley General.
Los sujetos obligados no podrán emitir acuerdos de carácter general ni particular que clasifiquen documentos o expedientes como reservados, ni clasificar documentos antes de dar respuesta a una solicitud de acceso a la información.
La clasificación de información reservada se realizará conforme a un análisis caso por caso, mediante la aplicación de la prueba de daño."

[5] ***"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.
A efecto de instituir un vínculo de comunicación para las gestiones derivadas de trámites de acceso a la información, protección de información reservada y/o confidencial y transparencia, los titulares de las instancias designarán un servidor público que fungirá como Enlace e informarán por escrito sobre su designación a la Unidad General."

[6] *"**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;
II. Recabar las necesidades de bienes y servicios en materia de tecnologías de la información y comunicación (…)
V. Planificar, diseñar, desarrollar y mantener en operación los sistemas informáticos jurídicos, administrativos y jurisdiccionales, así como los portales y micrositios que requieran los órganos y áreas, de conformidad con las disposiciones jurídicas aplicables;
VI. Elaborar estudios técnicos en materia de infraestructura tecnológica, así como de sistemas y bienes informáticos;
(…)
IX. Instrumentar los mecanismos en materia de seguridad informática y vigilar su adecuado funcionamiento;
(…)

[7] *"**Artículo 113.** Como información reservada podrá clasificarse aquella cuya publicación:*
(…)
VII. Obstruya la prevención o persecución de los delitos;"
(…)

nosXVDDVmmAajYnub+SVoigz3by7vwgi5YYS9wAmkOM=

General de Transparencia, de contenido idéntico a la fracción VII, del artículo 110 de la Ley Federal de Transparencia[8], para mantener la reserva de las políticas de seguridad implementadas para la prevención y solución de amenazas conforme a cada elemento para la protección de los sistemas informáticos de este Alto Tribunal.

Lo anterior es así, porque como lo sostiene Tecnologías de la Información, la divulgación de dicha información representa un riesgo real y demostrable de perjuicio al interés público, en tanto que colocaría a este Alto Tribunal en un estado de vulnerabilidad, facilitando actos como intervención de las comunicaciones, robo de datos y afectación a su infraestructura tecnológica.

El interés en proteger la información es mayor que el de divulgarla, porque como lo señala Tecnologías de la Información, con su divulgación se podría facilitar la comisión de delitos informáticos y se pondría en riesgo la seguridad de los sistemas, además de afectar la confianza de las personas justiciables que acuden a este Alto Tribunal.

Aunado a ello, la reserva de la información es una medida proporcional y necesaria para prevenir delitos informáticos, pues la instancia vinculada informa que se refiere a aspectos técnicos relacionados con la infraestructura tecnológica y de sistemas de este Alto Tribunal, incluso, que el acceso a dicha información permitiría que cualquier persona capacitada cometa algún ilícito al revelar detalles técnicos sobre los protocolos de seguridad y características de la infraestructura instalada.

nosXVDDVmmAajYnub+SVojgz3by7vwgi5YYS9wAmkOM=

---

[8] *"**Artículo 110.** Como información reservada podrá clasificarse aquella cuya publicación:*
(…)
***VII.** Obstruya la prevención o persecución de los delitos;"*
(…)

Conforme a lo expuesto, este Comité concluye que aún no es viable la divulgación de 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, lo cual fue materia de reserva en la resolución CT-CI/A-7-2020, ya que pondría en riesgo la seguridad de la infraestructura tecnológica de este Alto Tribunal y facilitaría la extracción, modificación o alteración de información contenida en sistemas o equipos informáticos.

Con base en lo expuesto, de conformidad con los artículos 44, fracción VIII[9], y 103[10], de la Ley General de Transparencia, se determina justificado ampliar el periodo de reserva, pues se trata de información que al divulgarla podría comprometer la seguridad de la infraestructura tecnológica de este Alto Tribunal, lo que tiene sustento en los artículos 113, fracción VII, de la Ley General de Transparencia y 110, fracción VII, de la Ley Federal de Transparencia.

Acerca del plazo por el que se ampliará la reserva de la información, se tiene en cuenta que el artículo 101[11] de la Ley General de

nosXVDDVmmAajYnub+SVojgz3by7vwgi5YYS9wAmkOM=

---

[9] *"**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"
(…)

[10] *"**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."

[11] ***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 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 Título.
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.

Transparencia contempla la posibilidad de que pueda ser hasta por cinco años.

En ese sentido, dado que se estima que prevalecen las causas que dieron origen a la reserva de la información referida, se estima justificado que el plazo se amplie por cinco años, contados a partir del vencimiento del primer periodo, en el entendido de que podrá concluir previamente, siempre que se actualice alguno de los supuestos de publicidad previstos en el artículo 101 de la Ley General de Transparencia.

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 y a la Unidad General de Transparencia.

Por unanimidad de votos lo resolvió el Comité de Transparencia de la Suprema Corte de Justicia de la Nación, integrado por el licenciado Mario José Pereira Meléndez, Director General de Asuntos Jurídicos y Presidente del Comité, maestro Christian Heberto Cymet López Suárez, Contralor del Alto Tribunal, y licenciado Adrián González Utusástegui,

nosXVDDVmmAajYnub+SVojgz3by7vwgi5YYS9wAmkOM=

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."

Titular de la Unidad General de Investigación de Responsabilidades Administrativas; quienes firman con la secretaria del Comité que autoriza.

LICENCIADO MARIO JOSÉ PEREIRA MELÉNDEZ
PRESIDENTE DEL COMITÉ

MAESTRO CHRISTIAN HEBERTO CYMET LÓPEZ SUÁREZ
INTEGRANTE DEL COMITÉ

LICENCIADO ADRIÁN GONZÁLEZ UTUSÁSTEGUI
INTEGRANTE DEL COMITÉ

MAESTRA SELENE GONZÁLEZ MEJÍA
SECRETARIA DEL COMITÉ

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

nosXVDDVmmAajYnub+SVojgz3by7vwgi5YYS9wAmkOM=