



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

**CUMPLIMIENTO CT-CUM/A-32-
2026, DERIVADO DEL DIVERSO
CT-CI/A-7-2021**

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 **veinticinco de junio de dos mil veintiséis**.

ANTECEDENTES:

PRIMERO. Solicitud de información. El diez de junio dos mil veintiuno, se recibió la solicitud de acceso a la información registrada en la Plataforma Nacional de Transparencia con el folio **0330000102821**, en la que se pidió lo siguiente:

“SOLICITO SABER SI UTILIZAN FIRMA ELECTRÓNICA, DE SER ASÍ, EN QUÉ DOCUMENTOS LA UTILIZAN, QUE ME PROPORCIONEN LA NORMATIVA QUE LES ES APLICABLE EN MATERIA DE FIRMA ELECTRÓNICA, QUE ME INDIQUEN CUÁL ES LA INFORMACIÓN QUE SE MUESTRA EN SU CÓDIGO FUENTE Y EL FUNDAMENTO LEGAL.”

SEGUNDO. Resolución del Comité de Transparencia en la que se clasificó la información: En sesión de siete de julio 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-7-2021**¹, en la cual determinó, en la parte que interesa, lo siguiente:

“[...]

II. Información reservada.

Por cuanto a hace [sic] al planteamiento señalado en el punto 3, relativo a conocer ‘cuál es la información que se muestra en su código fuente’, la Dirección General de Tecnologías de la Información lo clasifica como reservado, aduciendo que con su acceso se ponen en riesgo los sistemas de datos de este Alto Tribunal, porque se daría a conocer información técnica sobre los protocolos de seguridad y las características de la

¹ Consultable en: <https://www.scjn.gob.mx/sites/default/files/resoluciones/2021-08/CT-CI-A-7-2021.pdf>

infraestructura instalada, entre otros factores que se mencionarán más adelante.

‘[...]’

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.
- 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.

Como se señaló, la **reserva** de la información se fundamenta en el artículo 110, fracción VII, de la Ley Federal de Transparencia, en virtud de que su divulgación pondría en riesgo cuestiones de seguridad y conectividad de los sistemas informáticos y bases de datos de la Suprema Corte de Justicia de la Nación y 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 los artículos 2, fracción XXXVII y 5 del Acuerdo General de Administración II/2014, es responsable en la Suprema Corte de Justicia de la Nación de los sistemas informáticos de los que se pide 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 resulta aplicable 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 tiene 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 Pública y Protección de Datos personales (INAI) 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



argumentó 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 pudiera ‘obstruir la prevención de los delitos’, debe de 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 que *‘por definición de la palabra **prevención** se hace referencia a medidas y acciones dispuestas con anticipación con el fin de evitar o impedir que se presente un fenómeno peligroso para reducir sus efectos sobre la publicación’*, de ahí que prevención del delito significa *‘tomar medidas y realizar acciones para evitar una conducta o un comportamiento que puedan dañar o convertir a la población en sujetos o víctimas de un ilícito’* 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).

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

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-2-2019, este Comité de Transparencia **confirma la clasificación de reserva** de la *‘información que se muestra en su código de fuente’*, 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, la Dirección General de Tecnologías de la Información

como área técnica, ha expuesto los argumentos sobre la naturaleza de la información solicitada y dicha área señaló que al entregar esa información se podría comprometer la seguridad informática de los sistemas y equipos de este Alto Tribunal, porque se pondría en riesgo la seguridad operativa de la infraestructura tecnológica que permite la operación de las diversas áreas de la Suprema Corte de Justicia de la Nación.

Así, tomando en consideración la argumentación sostenida en la resolución del Instituto Nacional de Transparencia que se ha citado, 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 divulgar 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 [sic] 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 de lo contrario se pondría en riesgo la responsabilidad fundamental del Alto Tribunal en la defensa del orden establecido en la Constitución Federal, mediante sus funciones jurisdiccionales de carácter constitucional, así como las actuaciones administrativas que realizan los órganos y áreas de la Suprema Corte.

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 del información requerida sobre dicho aspecto en la solicitud implica llevar a cabo la prevención del delito de acceso ilícito a sistemas y equipos de informática tipificado en el Código Penal Federal, lo cual cobra importancia si se considera que dicha conducta implica conocer, copiar, modificar, destruir o provocar la pérdida de información contenida en sistemas o equipos de informática, por lo que revelar los datos que se muestran en el código fuente *'no sólo se comprometería la información que obra en los archivos digitales del sujeto obligado, sino que menoscabaría la seguridad y certeza de los ciudadanos que acuden a éste para otorgar certeza respecto de la impartición de justicia y control constitucional'*.

Ahora bien, dicha clasificación de reserva **'se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio, toda vez que la pretensión de fondo que persigue la reserva de la información consiste en prevenir la conducta antijurídica tipificada (acceso ilícito a sistemas y equipos de informática)'**,



de llevarse a cabo podría permitir la ejecución de diversos **ataques** a la infraestructura tecnológica y de sistemas con que cuenta este Alto Tribunal, ya que la difusión de 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 acorde con las consideraciones expuestas en la resolución del Instituto Nacional de Transparencia a que se hace mención y en la de cumplimiento CT CUM-R/A-2-2019 de este Comité, ***‘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,

RESUELVE:

[...]

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 **CT-219-2026** de cinco de junio dos mil veintiséis, la Secretaria del Comité de Transparencia solicitó a la persona titular de la **Dirección General Tecnologías de la Información** (en lo sucesivo **DGTI**) de la Unidad de Administración de la Suprema Corte de Justicia de la Nación que emitiera un informe sobre la vigencia del plazo de clasificación de la información reservada, a que se refirió la resolución de este Comité de Transparencia identificada como **CT-CI/A-7-2021**, en el que precisara si el plazo de reserva era susceptible de ampliarse (indicando las razones y fundamento legal), o bien, si procedería su desclasificación (en tanto que habría transcurrido el plazo de clasificación).

CUARTO. Informe de la DGTI. Por oficio **UASCJN/DGTI/DAN-127-2026** de diez de junio de dos mil veintiséis, el Enlace de Transparencia de esa Dirección General remitió la Nota **UASCJN/DGTI/SGSIC-I-9-2026**, por la que

el Subdirector General de Seguridad Informática y Ciberseguridad 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 del código fuente, se informa que subsisten las causas que dieron origen a la clasificación de la información como reservada, con fundamento en los artículos 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública (se inserta vínculo electrónico para consulta y en adelante Ley Federal de Transparencia); y 113, fracción VII, de la Ley General de Transparencia y Acceso a la Información Pública (se inserta vínculo electrónico para consulta y en adelante Ley General de Transparencia), ambas legislaciones vigentes al momento de la presentación de la solicitud de acceso la información (diez de junio de dos mil veintiuno), ya que su divulgación:

- Permitiría el acceso ilícito a sus sistemas y equipos informáticos, intentando la suplantación de estos;
- Potenciaría la posibilidad de vulnerar la seguridad de si infraestructura tecnológica;
- Establecería con un alto grado de precisión la información técnica referente a los protocolos de seguridad y las características de la infraestructura instalada;
- Pondría en un estado vulnerable a la institución, facilitando la intervención de las comunicaciones y permitiendo usurpar permisos requeridos en la red para obtener información;
- Daría a conocer puntos de vulnerabilidad para la seguridad de la infraestructura de cómputo;
- Vulneraría sus sistemas informáticos, así como la información contenida en éstos;
- Atentaría en contra de su infraestructura tecnológica, afectando el ejercicio de sus labores sustantivas; y
- Modificaría, destruiría o provocaría pérdida de información contenida en sus sistemas.

Asimismo, se advierte que la negativa de acceso a la información se motiva en pretender evitar o prevenir la comisión del delito de acceso ilícito a sus equipos y sistemas de informática.

Al respecto, el Código Penal Federal (se inserta vinculo electrónico para consulta) dispone lo siguiente:

‘Acceso ilícito y equipos de informática

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

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

ARTICULO 211 BIS 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del

bCV4RsF1103jsrpgF8VxFKMcZDWvPtW7ZIG4LF0FYw=



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.

Con base en lo anterior, el riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda la información, ya que el resguardo de los datos requeridos por el solicitante implica la prevención del delito de acceso ilícito a sistemas y equipos de informática tipificado en el Código Penal Federal, lo cual cobra importancia si se considera que dicha conducta implica conocer, copiar, modificar, destruir o provocar la pérdida de información contenida en sistemas o equipos de informática.

Asimismo, la limitación 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), misma que de llevarse a cabo podría permitir la realización de diversos ataques de la infraestructura tecnológica y de sistemas del sujeto obligado, los cuales podrían traer como consecuencia la inoperatividad de sus funciones, por un periodo indeterminado.

Por todo lo anterior, se advierte que difundir la información requerida incrementa sustancialmente la posibilidad de que aquella persona que conozca dicha información cometa algún ilícito, accediendo de forma no autorizada a los sistemas de datos que no son públicos en posesión del sujeto obligado, conociendo con un alto grado de precisión la información

técnica referente a sus equipos de cómputo, 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 Ley Federal de Transparencia (se inserta vínculo electrónico para consulta) y la fracción VII del artículo 113 de la Ley General de Transparencia (se inserta vínculo electrónico para consulta).

Ahora bien, en cuanto al periodo de reserva, el artículo 99 de la Ley Federal de Transparencia (se inserta vínculo electrónico para consulta), así como el Trigésimo Cuarto de los Lineamientos Generales (se inserta vínculo electrónico para consulta), 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 (se inserta vínculo electrónico para consulta).

Por último, todo lo anteriormente expuesto se refuerza con lo resuelto por el Comité de Transparencia a través del expediente cumplimiento [sic] CUMPLIMIENTO CT-CUM/A-6-2026, DERIVADO DEL DIVERSO CT-CI/A-2-2021 (se inserta vínculo electrónico para consulta) y CUMPLIMIENTO CT-CUM/A-47-2023 (se inserta vínculo electrónico para consulta).
[...]"

QUINTO. Acuerdo de turno. Por proveído de diez de junio de dos mil veintiséis, la Presidenta del Comité de Transparencia 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 (DOF) el cuatro de mayo del dos mil quince, así como 27 del Acuerdo General de Administración 5/2015, integró y registró el presente expediente y ordenó su remisión a la persona titular de la Dirección General 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 notificó mediante oficio **CT-253-2026** de esa misma fecha.

CONSIDERANDO:

PRIMERO. Consideración Previa.

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”, en cuyo artículo Segundo Transitorio², 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).

No obstante lo anterior, los artículos Noveno y Décimo³ transitorios del propio Decreto disponen que **todos aquellos procedimientos iniciados con**

² “**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;

[...]

³ “**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.

[...]

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 sustanciaran** 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 **0330000102821** fue presentada en la Plataforma Nacional de Transparencia el **diez de junio 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 realizaran conforme a la legislación abrogada pero aplicable al caso en concreto.

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 (diez de junio de dos mil veintiuno), conservando de esta manera la validez, competencia y efectos jurídicos de este procedimiento.

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.

[...]"



SEGUNDO. Competencia. 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 y Acceso a la Información Pública, así como 23, fracciones I y II, del Acuerdo General de Administración 5/2015, este Comité de Transparencia de la Suprema Corte de Justicia de la Nación es legalmente competente para pronunciarse sobre la ampliación del periodo de reserva de la información.

TERCERO. Análisis. En la solicitud que da origen a este asunto, se requirió información relacionada con la utilización, normativa, código fuente y fundamento legal de la Firma Electrónica (FIREL), sobre lo cual, en la resolución **CT-CI/A-7-2021**⁴, se determinó que de conformidad con los artículos 110, fracción VII, de la Ley Federal de Transparencia⁵, y 113, fracción VII, de la Ley General de Transparencia⁶, la información relativa al código fuente de la firma electrónica (FIREL) era considerada como **reservada**.

Debido a que el plazo de reserva de la información se encuentra próximo a vencer, la Secretaria de este Comité de Transparencia requirió a la **DGTI** para que se pronunciara sobre la vigencia de la reserva de la información antes señalada, o bien, si procedía su desclasificación.

Bajo ese tenor, mediante la Nota **UASCJN/DGTI/SGSIC-I-9-2026**, transcrita en el antecedente CUARTO de la presente determinación, la **DGTI** indicó que **aún persisten las causas para clasificar como reservada la**

⁴ Consultable en: <https://www.supremacorte.gob.mx/sites/default/files/resoluciones/2021-08/CT-CI-A-7-2021.pdf>

⁵ “**Artículo 110.** Conforme a lo dispuesto por el artículo 113 de la Ley General, como información reservada podrá clasificarse aquella cuya divulgación:

[...]

VII. Obstruya la prevención o persecución de los delitos;

[...]”.

⁶ “**Artículo 113.** Como información reservada podrá clasificarse aquella cuya publicación:

[...]

VII. Obstruya la prevención o persecución de los delitos;

[...]”.

información relativa al código fuente de la Firma Electrónica (FIREL), bajo los siguientes argumentos:

- La divulgación de la información establecería con gran precisión la información técnica o puntos de vulnerabilidad de los protocolos de seguridad y las características de la infraestructura.
- Se permitiría que, con mayor facilidad, se pudiera tener un acceso ilícito a los sistemas y equipos informáticos de la Suprema Corte de Justicia de la Nación, o bien, la intervención de las comunicaciones, potenciando una vulneración en la seguridad de los sistemas e infraestructura tecnológicos.
- Se supera al interés público de que se difunda la información, toda vez que el resguardo de la información conlleva a la prevención del delito de acceso ilícito a sistemas y equipos de informática, tipificado en el Código Penal Federal, el cual implica que se conozcan, copien, modifiquen, destruyan o se provoque la pérdida de información contenida en sistemas o equipos de informática.
- La reserva se adecua al principio de proporcionalidad y representa el medio menos restrictivo para evitar el perjuicio, en virtud de que se previene una conducta antijurídica, que, de llevarse a cabo, posibilitaría la realización de ataques informáticos, lo que traería como consecuencia la inoperatividad de la infraestructura tecnológica.

Para determinar la procedencia de la ampliación del plazo de reserva de la información materia del presente asunto, debe considerarse que, de conformidad con los artículos 100, párrafo tercero, de la Ley General de Transparencia⁷ y 97, párrafo tercero, de la Ley Federal de Transparencia⁸, en correlación con el diverso 17 del Acuerdo General de Administración 5/2015⁹, corresponde a las personas titulares de las áreas que tienen bajo resguardo

⁷ **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.”

⁸ **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.”

⁹ **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.

[...]”



la información solicitada, determinar su disponibilidad y, en su caso, clasificarla conforme a la normativa aplicable.

En ese sentido, en el presente caso, la **DGTI** es el área competente para pronunciarse respecto de la ampliación del plazo de reserva, toda vez que, como se estableció en la citada resolución **CT-CI/A-7-2021**, es el área responsable de los sistemas informáticos en la Suprema Corte de Justicia de la Nación sobre los cuales se solicita la información.

En términos de lo señalado por la **DGTI**, la divulgación de la información consistente en el código fuente de la FIREL representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público, superando el interés de que la información sea revelada, y por lo tanto, la reserva de la información representa el medio menos restrictivo para evitar el perjuicio que significaría dar a conocer la información requerida.

Por lo tanto, este Comité de Transparencia considera que se encuentra justificada la ampliación del plazo de reserva, toda vez que, de los argumentos vertidos por el área vinculada, se desprende que:

- La difusión de los datos requeridos tiene el potencial de vulnerar los sistemas tecnológicos de esta Suprema Corte, dando a conocer información específica de la infraestructura con la que se cuenta, y con ello, se posibilita el ingreso a los sistemas informáticos, lo cual constituye un delito de orden federal, sobre el cual se tiene el deber de prevenirlo y evitarlo.
- En caso de que se permita el acceso a la información requerida, se podría tener como consecuencia la realización de ataques en contra de la infraestructura tecnológica, y con ello, no solo se vulnera la seguridad de los sistemas, sino de la información que en ellos se contiene.
- No solo se comprometen aquellos archivos administrativos que contienen información personal y sensible de trabajadores y proveedores, sino 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, la divulgación de la información solicitada podría revelar datos que funcionarían como herramienta indirecta para facilitar el acceso no autorizado a los sistemas y equipos de informática con los cuales cuenta esta Institución, poniendo en una situación de evidente riesgo la seguridad Institucional, toda vez que ello permitiría, entre otros supuestos:

- La extracción y divulgación de información de la cual esta Suprema Corte de Justicia de la Nación tiene el deber de salvaguardar protección (como lo son políticas de seguridad institucional o información sensible otorgada a la Institución).
- La modificación o destrucción de información que coadyuva a que esta Suprema Corte cumpla con su deber jurisdiccional constitucional, así como aquella que sirve de sustento para realizar sus funciones administrativas.

Al considerarse que la divulgación de la información permitiría el ingreso a los sistemas con los que cuenta este Tribunal Constitucional, se considera aplicable por analogía lo sustentado en el expediente **CT-CUM/A-52-2023**¹⁰, en el sentido de que el daño que se podría producir con la divulgación de la información relativa al código fuente de la FIREL “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 expediente **CT-CUM/RA-2-2019**¹¹, en el cual se determinó 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;

¹⁰ Disponible en: <https://www.scjn.gob.mx/sites/default/files/resoluciones/2023-11/CT-CUM-A-52-2023.pdf>

¹¹ Disponible en: <https://www.scjn.gob.mx/sites/default/files/resoluciones/2019-03/CT-CUM-R-A-2-2019.pdf>



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 del código fuente 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 la realización de ataques.

En consecuencia, acorde con los artículos 44, fracción VIII¹², y 103¹³ 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-7-2021**, el siete de julio de dos mil veintiuno, al actualizarse la hipótesis prevista en la fracción VII¹⁴ 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.

Por lo expuesto, este Comité autoriza 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

¹² “**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

[...]”

¹³ “**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.”

¹⁴ Establecen que la información podrá ser clasificada como reservada cuando su publicación:

VII. Obstruya la prevención o persecución de los delitos.

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 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, 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**

**MAESTRO ABRAHAM MONTES MAGAÑA
INTEGRANTE DEL COMITÉ**

**DOCTOR GUSTAVO MIGUEL MEIXUEIRO NÁJERA
INTEGRANTE DEL COMITÉ**



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

CT-CUM/A-32-2026

**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.”

bCV4RsF1103jserpgF8VxFKMcZDWvPtW7ZIG4LF0FYw=