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

CLASIFICACIÓN DE INFORMACIÓN
CT-CI/A-7-2021

INSTANCIA REQUERIDA:
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 siete de julio de dos mil veintiuno.

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

I. Solicitud de información. El diez de junio de dos mil veintiuno, se recibió la solicitud tramitada en la Plataforma Nacional de Transparencia con el folio 0330000102821, requiriendo:

> *"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."*

II. Acuerdo de admisión de la solicitud. En acuerdo de once de junio de dos mil veintiuno, la Unidad General de Transparencia y Sistematización de la Información Judicial, por conducto de su Subdirector General, una vez analizada la naturaleza y contenido de la solicitud, con fundamento en los artículos 123 y 124, de la Ley General de Transparencia y Acceso a la Información Pública, 124 y 125, de la Ley Federal de Transparencia y Acceso a la Información Pública y 7 del

Acuerdo General de Administración 5/2015, la estimó procedente y ordenó abrir el expediente UT-A/0187/2021.

En el mismo acuerdo se señaló que con independencia de las gestiones realizadas para atender la solicitud de acceso, en la respuesta que se proporcionara a la persona solicitante se hiciera del conocimiento las ligas electrónicas en que se puede consultar la *"Solicitud de Certificado Digital de Firma Electrónica, así como del Acuerdo General Plenario número 9/2020, el cual regula la integración de los expedientes electrónico e impreso, así como el uso del Sistema Electrónico de la Suprema Corte de Justicia de la Nación"*

III. Requerimiento de información. El Titular de la Unidad General de Transparencia y Sistematización de la Información Judicial, a través del oficio UGTSIJ/TAIPDP/1755/2021, enviado mediante comunicación electrónica de quince de junio de dos mil veintiuno, solicitó a la Dirección General de Tecnologías de la Información que se pronunciara sobre la existencia y clasificación de la información materia de la solicitud.

IV. Informe de la Dirección General de Tecnologías de la Información. El veintitrés de junio de dos mil veintiuno, se recibió en la cuenta de correo electrónico habilitada para tales efectos por la Unidad General de Transparencia, el oficio DGTI/281/2021, con el que la titular de esa dirección general remite la "Atenta Nota de Cumplimiento con números SGSI-I/21/2021 y DGTI/DSI/09/2021", suscrita por la Directora de Sistemas Jurídicos, el Director de Seguridad Informática y el Subdirector de Gobierno de Seguridad de la Información, la cual se transcribe enseguida:

*"**RESPUESTA A SOLICITUD***
Sí, se usa Firma Electrónica en documentos jurídicos y administrativos, la normativa aplicable a la Firma Electrónica (FIREL), es la siguiente:

- ✓ *Acuerdo General Conjunto Número 1/2013, de la Suprema Corte de Justicia de la Nación, del Tribunal Electoral del Poder Judicial de la Federación y del Consejo de la Judicatura Federal, relativo a la Firma Electrónica Certificada del Poder Judicial de la Federación (FIREL) y al Expediente Electrónico;*

- ✓ *Las Políticas para la Obtención y uso de la Firma Electrónica Certificada del Poder Judicial de la Federación (FIREL), así como para la Operación de su Infraestructura Tecnológica.*

- ✓ *Acuerdo General de Administración II/2014 (AGA II/2014), de diecinueve de agosto de dos mil catorce, del Comité de Gobierno y Administración, por el que se regula el uso de la Firma Electrónica Certificada del Poder Judicial de la Federación (FIREL), en la Suprema Corte de Justicia de la Nación.*

- ✓ *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, por el que se regula el trámite electrónico y uso de la Firma Electrónica Certificada del Poder Judicial de la Federación (FIREL) para actuaciones administrativas."*

En el marco de los principios rectores del procedimiento de acceso a la información y siendo ésta pública, la normatividad antes referida puede ser consultada en la página de internet de la Suprema Corte de Justicia de la Nación en los siguientes vínculos electrónicos:

- *https://www.scjn.gob.mx/sites/default/files/acuerdos_generales/documento/2016-11/Acuerdo%20General%20Conjunto1-2013%20%28FIREL%29%20Versi%C3%B3n%20Aprobada_1.pdf*

- *https://www.pjf.gob.mx/Docs/Politicas%20Firel%20con%20rubricas%20y%20firmas.pdf*

- *AGAII-2014FIRMAELECTRONICACERTIFICADA https://www.scjn.gob.mx/sites/default/files/marco-normativo/disposiciones-caracter-gral-expedidas-scjn/acuerdos-administrativos/documento/2016-12/AGA%20II-2014%20FIRMA%20ELECTRONICA%20CERTIFICADA.pdf.pdf(scjn.gob.mx)*

- *https://www.scjn.gob.mx/conoce-la-corte/marconormativo/public/api/download?fileName=aga%20III-*

20%20tramite-electronico-uso-firel-actuaciones-administrativas-scjn.pdf

Por lo que respecta al código fuente, se comunica que la información solicitada se considera reservada, de conformidad con lo dispuesto en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, ya que la divulgación de la misma:

- *Permitiría el acceso ilícito a sus sistemas y equipos informáticos, intentando la suplantación de los mismos;*
- *Potenciaría la posibilidad de vulnerar la seguridad de su 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.*

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 dispone lo siguiente:

> ***Acceso ilícito a sistemas y equipos de informática***
> ***Artículo 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.*
> ***Artículo 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 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 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.*
> *…*
> ***Artículo 211 bis 7.-** Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.*

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

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

V. Vista a la Secretaría del Comité de Transparencia. Mediante correo electrónico de veintiocho de junio de dos mil veintiuno, el Titular de la Unidad General de Transparencia y Sistematización de la Información Judicial remitió el oficio UGTSIJ/TAIPDP/1980/2021 y el

expediente electrónico UT-A/0187/2021 a la Secretaría del Comité de Transparencia, con la finalidad de que se dictara la resolución correspondiente.

VI. Acuerdo de turno. Mediante acuerdo de veintiocho de junio de dos mil veintiuno, la Presidencia del Comité de Transparencia, con fundamento en los artículos 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública, así como 23, fracción II, y 27, del Acuerdo General de Administración 5/2015, ordenó integrar el expediente **CT-CI/A-7-2021** y, conforme al turno correspondiente, remitirlo al Contralor del Alto Tribunal, a fin de que presentara la propuesta de resolución, lo que se hizo mediante oficio CT-300-2021, enviado mediante correo electrónico en esa misma fecha.

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

PRIMERO. Competencia. El Comité de Transparencia de la Suprema Corte de Justicia de la Nación es competente para conocer y resolver el presente asunto, en términos de lo dispuesto en los artículos 6° de la Constitución Política de los Estados Unidos Mexicanos, 4 y 44, fracciones II y III, de la Ley General de Transparencia y Acceso a la Información Pública, 65, fracciones II y III, de la Ley Federal de Transparencia y Acceso a la Información Pública, así como 23, fracciones II y III, del Acuerdo General de Administración 5/2015.

SEGUNDO. Análisis. En la solicitud se pide conocer: 1) si se utiliza firma electrónica y en qué documentos; 2) la normativa que es aplicable y, 3) cuál es la información que se muestra en el código fuente y el fundamento legal.

I. Información que se pone a disposición.

Por cuanto a la información que se señala en el punto 1, en la nota conjunta de la Directora de Sistemas Jurídicos, el Director de Seguridad Informática y el Subdirector de Gobierno de Seguridad de la Información, remitida por la Directora General de Tecnologías de la Información, se informa que sí se hace uso de la Firma Electrónica Certificada del Poder Judicial de la Federación (FIREL) en documentos jurídicos (jurisdiccionales) y administrativos; además, se precisa la normativa que regula el uso de la FIREL, con lo cual se da respuesta al punto 2 de la solicitud, siendo la siguiente:

- “Acuerdo General Conjunto Número 1/2013, de la Suprema Corte de Justicia de la Nación, del Tribunal Electoral del Poder Judicial de la Federación y del Consejo de la Judicatura Federal, relativo a la Firma Electrónica Certificada del Poder Judicial de la Federación (FIREL) y al Expediente Electrónico”.

- “Las Políticas para la Obtención y uso de la Firma Electrónica Certificada del Poder Judicial de la Federación (FIREL), así como para la Operación de su Infraestructura Tecnológica”.

- “Acuerdo General de Administración II/2014 (AGA II/2014), de diecinueve de agosto de dos mil catorce, del Comité de Gobierno y Administración, por el que se regula el uso de la Firma Electrónica Certificada del Poder Judicial de la Federación (FIREL), en la Suprema Corte de Justicia de la Nación”.

- “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, por el que se regula el trámite electrónico y uso de la Firma Electrónica Certificada del Poder Judicial de la Federación (FIREL) para actuaciones administrativas”, proporcionando las ligas de internet en que se pueden consultar esos instrumentos normativos.

Dada la materia de la solicitud, se debe adicionar a la lista proporcionada por la Dirección General de Tecnologías de la Información, el Acuerdo General De Administración número V/2020 del Presidente de la Suprema Corte de Justicia de la Nación, de nueve de octubre de dos mil veinte, por el que se establecen reglas para el trámite electrónico de los procedimientos de responsabilidad administrativa, el cual puede consultarse en la liga Suprema Corte de Justicia de la Nación (scjn.gob.mx)

Aunado a lo anterior, se hace notar que en el acuerdo de admisión de la solicitud, la Unidad General de Transparencia hizo saber al solicitante las ligas electrónicas en que se puede consultar la “Solicitud de Certificado Digital de Firma Electrónica” y el “Acuerdo General Plenario número 9/2020, el cual regula la integración de los expedientes electrónico e impreso, así como el uso del Sistema Electrónico de la Suprema Corte de Justicia de la Nación”.

Por otra parte, en la solicitud se pide el fundamento legal del código fuente, respecto de lo cual, si bien el área requerida no hizo un pronunciamiento específico al respecto, también es cierto que proporcionó la lista de los ordenamientos aplicables sobre la firma electrónica al señalar que sí se contaba con ésta; de ahí que no es

necesario requerir que haga esa precisión, puesto que se estima atendido ese aspecto al informar el nombre de los instrumentos normativos que son aplicables sobre la firma electrónica tanto en el ámbito jurisdiccional como administrativo.

Conforme a lo expuesto, se estima que con la información proporcionada tanto por la Dirección General de Tecnologías de la Información, como por la Unidad General de Transparencia se atienden los aspectos planteados en la solicitud que se identifican en esta resolución con los números 1, 2 y 3 (en cuanto al fundamento legal del código fuente) y, por tanto, se encomienda a la citada Unidad General de Transparencia que haga del conocimiento de la persona solicitante lo informado al respecto.

II. Información reservada.

Por cuanto a hace 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 infraestructura instalada, entre otros factores que se mencionarán más adelante.

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[1].

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.

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:

---

[1] ***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)*

- Permitiría el acceso ilícito a los sistemas y equipos, ejerciendo la suplantación de éstos.
- 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[2], 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 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 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*

---

[2] *"Artículo 2o. Para efectos del presente instrumento normativo, se entenderá por:*
(…)
XXXVII. Unidad de Certificación de la SCJN: La DGTI, responsable de llevar a cabo los procedimientos para su emisión, renovación, revocación y consulta, por sí o, en los términos de la normativa aplicable, por conducto de los agentes certificadores adscritos a la Secretaría General de Acuerdos, respecto de los Justiciables y del área que designe el titular de la Oficialía Mayor, respecto de los servidores públicos de la SCJN.
(…)
Artículo 5o. La Autoridad Certificadora de la SCJN ejecutará, en términos de las disposiciones aplicables en el presente instrumento normativo, los procedimientos para el registro de datos y verificación de elementos de identificación, emisión, renovación y revocación de certificados digitales de la FIREL; además, administrará la infraestructura tecnológica de la FIREL, establecerá los controles de accesos, respaldos y recuperación de información, así como los mecanismos confiables de seguridad, disponibilidad, integridad, autenticidad, confidencialidad y custodia."

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 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 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[3], 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 hacho 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,

---

[3] ***"Artículo 101.*** *Los Documentos clasificados como reservados serán públicos cuando:*
…
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…"

R E S U E L V E:

PRIMERO. Se tiene por atendida la solicitud por cuanto a la información mencionada en el considerando segundo, apartado I, 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.

Notifíquese al solicitante, a la instancia requerida 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 maestro Luis Fernando Corona Horta, Director General de Asuntos Jurídicos y Presidente del Comité, Maestro Christian Heberto Cymet López Suárez, Contralor del Alto Tribunal, y Maestro Julio César Ramírez Carreón, Titular de la Unidad General de Investigación de Responsabilidades Administrativas; quienes firman con el secretario del Comité que autoriza.

MAESTRO LUIS FERNANDO CORONA HORTA
PRESIDENTE DEL COMITÉ

MAESTRO CHRISTIAN HEBERTO CYMET LÓPEZ SUÁREZ
INTEGRANTE DEL COMITÉ

MAESTRO JULIO CÉSAR RAMÍREZ CARREÓN
INTEGRANTE DEL COMITÉ

LICENCIADO ARIEL EFRÉN ORTEGA VÁZQUEZ
SECRETARIO 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."