CLASIFICACIÓN DE INFORMACIÓN CT-CI/A-1-2019

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 treinta de enero de dos mil diecinueve.

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

I. Solicitud de información. El diez de diciembre de dos mil dieciocho, se recibió en la Plataforma Nacional de Transparencia la solicitud tramitada con el folio 0330000229718, requiriendo:

> *"Con fundamento en el artículo 6 constitucional, atentamente requiero que en función de los principios constitucionales de máxima publicidad, transparencia, rendición de cuentas y gratuidad, me entregue a través de un medio gratuito derivado de los avances tecnológicos y en formato de documento portátil (PDF) comprimido o en diverso de naturaleza similar, la siguiente información pública documentada en el ejercicio de las facultades, competencias y funciones previstas en las normas jurídicas aplicables.*
>
> 1. *Por número de serie de cada uno de los equipos de cómputo en posesión del sujeto obligado requiero:*
>   a) *Nombres comerciales de los sistemas operativos instalados.*
>   b) *Nombres comerciales y versiones de los antivirus o software de seguridad en Internet, instalados.*
>   c) *Inicio y termino de la vigencia de cada licencia utilizada en los software mencionados en el anterior inciso b).*
>
> 2. *Por dirección web o URL (Localizador Uniforme de Recursos), de los protocolos HTTP (Protocolo de transferencia de Hipertexto) y HTTPS (Protocolo seguro de transferencia de hipertexto), cuál es utilizado en cada una de sus páginas electrónicas o webs oficiales, así como el tipo de protocolo de seguridad implementado, SSL (Capa de sockets seguros) o TLS (Seguridad de la capa de transporte).*
>
> 3. *De cada una de sus actuales páginas electrónicas o webs oficiales, fecha exacta y duración de todos los ataques de Denegación de Servicio (DoS) o Denegación de Servicio Distribuida (DDoS) padecidos."*

II. Acuerdo de admisión de la solicitud. En acuerdo de diez de diciembre de dos mil dieciocho, 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/0514/2018 (foja 4)

III. Requerimiento de información. Por oficio UGTSIJ/TAIPDP/3380/2018, el diez de diciembre de dos mil dieciocho, el Titular de la Unidad General de Transparencia y Sistematización de la Información Judicial solicitó a la Dirección General de Tecnologías de la Información se pronunciara sobre la existencia y clasificación de la información materia de la solicitud (foja 5).

IV. Respuesta de la Dirección General de Tecnologías de la Información. El dos de enero de dos mil diecinueve, se recibió en la Unidad General de Transparencia el oficio DGTI/DAPTI-2925-2018, en el que se informa lo siguiente (fojas 6 a 8):

(…)

"Hago referencia a diversas solicitudes, así como resoluciones tanto del Comité de Transparencia como del INAI que están directamente relacionadas a la presente, en todos los casos solicitan se proporcione información diversa de aspectos propios de la infraestructura tecnológica y de seguridad con la que esta SCJN cuenta, cabe señalar que en todos los casos se reservó la información:

- *CT-CI/A-3-2018 de la Octava Sesión Pública Ordinaria celebrada el dieciocho de abril del año en curso.*
- *CT-CI/A-5-2018 de la Novena Sesión pública Ordinaria celebrada el dos de mayo del año en curso.*
- *CT-CI/A-11-2018 de la Décima Tercera Sesión Pública Ordinaria celebrada el veintisiete de junio del año en curso.*

- *CT-CUM-R/A-2/2018 en Resolución del Comité de Transparencia de la SCJN el cinco de diciembre del año en curso, en el que se informa la resolución del INAI.*

De lo anterior, se desprende que proporcionar cualquier dato o elemento que lleve a obtener información de:

- *Acceso a los canales de comunicación de este Alto Tribunal*
- *Aspectos de seguridad que permiten resguardar la información relevante.*
- *Datos propios de la infraestructura tecnológica.*

A continuación, se listan de manera puntual los datos que el solicitante requiere en el presente requerimiento, los cuales son evidentemente de aspectos muy técnicos que solo un experto en la materia conoce y sabrá darle el uso que mejor le convenga, por lo que generan en sí un alto riesgo de vulnerabilidad:

- *Sistemas operativos instalados*
- *Nombres comerciales, versiones y vigencias de los antivirus o software de seguridad en Internet instalados*
- *Lista de las páginas web señalando el protocolo que utiliza (HTTP o HTTPS) y el tipo de seguridad implementado (SSL o TLS), así como las fechas y duración de los ataques de Denegación de Servicio (DoS) o Denegación de Servicio Distribuida (DDoS) padecidos.*

Asimismo, se puede advertir, que hay una constante insistencia del peticionario para conocer detalles de aspectos técnicos y específicos que darían a conocer la infraestructura y seguridad tecnológica de esta SCJN.

En las diversas respuestas de esta naturaleza, se ha planteado que cada elemento sirve para salvaguardar la información y comunicaciones que hacen uso del sistema de comunicaciones del Alto Tribunal, y proporcionar alguno de ellos podría poner en riesgo cuestiones de seguridad pública y, con ello, el acceso a la justicia. Asimismo, se pueden tener las siguientes consecuencias:

- *Suplantación de identidad para acceder a la red y a toda la infraestructura tecnológica y de comunicaciones, con lo que podría extraerse información sobre la conducción de los expedientes judiciales o procedimientos administrativos seguidos en forma de juicio que no hayan causado estado.*

- *Se expone la capacidad de reacción ante posibles ataques informáticos, porque se identificaría o remitiría información contenida en los equipos, servidores, equipos de comunicación, atentando la seguridad y conectividad tecnológica que se tiene implementada.*

- *La información requerida, en su conjunto, permite que cualquier persona capacitada ingrese a los sistemas de comunicación y a la información que se aloje en esos sistemas.*

- *Cualquier afectación al Alto Tribunal pondría de igual forma en riesgo a las otras dos instancias del PJF, teniendo como una cuestión de seguridad pública tanto para el PJF, como para los justiciables; ya que la red de comunicaciones de la SCJN, interconecta con los demás órganos del Poder Judicial de la Federación (CJF, Juzgados de Distrito, Tribunales Unitarios, Tribunales Colegiados y TEPJF).*

Por lo anterior, la información solicitada es clasificada como reservada, con fundamento en la Ley General de transparencia y Acceso a la Información Pública, en el Artículo 113, fracción I; ya que son datos que deben tratarse con mucha cautela y no pueden proporcionarse, debido a que ponen en riesgo la información contenida en los equipos de este Alto Tribunal, quedando altamente vulnerables y sin protección."

V. Vista a la Secretaría del Comité de Transparencia. El once de enero de dos mil diecinueve, el Titular de la Unidad General de Transparencia y Sistematización de la Información Judicial, a través del oficio UGTSIJ/TAIPDP/0150/2019, remitió el expediente UT-A/0514/2018 a la Secretaría del Comité de Transparencia, con la finalidad de que se dictara la resolución correspondiente.

VI. Acuerdo de turno. En proveído de quince de enero de dos mil diecinueve, la Presidenta del Comité de Transparencia de este Alto Tribunal, con fundamento en los artículos 44, fracción II de la Ley General de Transparencia y Acceso a la Información Pública, 23, fracción II y 27 del Acuerdo General de Administración 5/2015, ordenó integrar el expediente **CT-CI/A-1-2019** 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-40-2019 el dieciséis de enero de este año.

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

I. Competencia. El Comité de Transparencia de la Suprema Corte de Justicia de la Nación es competente para conocer y resolver el presente asunto, en términos de lo dispuesto en los artículos 6° de la Constitución Política de los Estados Unidos Mexicanos, 4 y 44, fracciones I, II y III de la Ley General de Transparencia y Acceso a la Información Pública, 65,

fracciones I, 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.

II. Análisis. En la solicitud se pide que, a partir del número de serie de cada uno de los equipos de cómputo, se informe sobre los sistemas operativos instalados, nombres comerciales, versiones y vigencias de los antivirus o software de seguridad instalados, listas de las páginas webs señalando el protocolo que se utiliza y el tipo de seguridad implementado, así como las fechas y duración de los ataques de “Denegación de Servicio” o de “Denegación de Servicio Distribuida padecidos”.

En respuesta a lo anterior, la Dirección General de Tecnologías de la Información clasifica la información como reservada, aduciendo que se pone en riesgo la información contenida en los equipos y sistemas de este Alto Tribunal, pudiendo quedar vulnerables y sin protección.

Para llevar a cabo el análisis correspondiente, se recuerda que en el esquema de nuestro sistema constitucional, el derecho de acceso a la información encuentra cimiento a partir de lo dispuesto en el artículo 6º, apartado A, de la Constitución Política de los Estados Unidos Mexicanos (Constitución), 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].

Así, precisamente en atención al dispositivo constitucional antes referido, se obtiene que la información que tienen bajo su resguardo los sujetos obligados del Estado encuentra como excepción aquella que sea temporalmente reservada o confidencial en los términos establecidos por el legislador federal o local, cuando de su propagación pueda derivarse perjuicio por causa de interés público y seguridad nacional.

Para sustentar la clasificación de reserva que hace la Dirección General de Tecnologías de la Información cita el artículo 113, fracción I de la Ley General de Transparencia, manifestando, substancialmente, lo siguiente:

- El “INAI” y este Comité de Transparencia han emitido diversas resoluciones[2] directamente relacionadas con la materia de la solicitud, reservando, en todos los casos, la información.
- Los datos requeridos en la solicitud corresponden a aspectos técnicos que solo un experto en la materia conoce y sabría darle el uso que mejor le convenga, generando, en su caso, un alto riesgo de vulnerabilidad.

[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)*

[2] CT-CI/A-3-2018; CT-CI/A-5-2018; CT-CI/A-11-2018; CT-CUM-R/A-2-2018

- Existe una insistencia de conocer detalles técnicos y específicos que publicitarían la infraestructura y seguridad tecnológica del Alto Tribunal.
- En las diversas respuestas de esta naturaleza se ha planteado que cada elemento sirve para salvaguardar la información y comunicaciones que hacen uso del sistema de comunicaciones del Alto Tribunal, por lo que dar a conocer alguno podría poner en riesgo cuestiones de seguridad pública y con ello el acceso a la justicia.
- Se puede ejercer la suplantación de identidad del equipo para acceder a la red y a toda la infraestructura tecnológica y de comunicaciones, pudiéndose extraer información sobre la conducción de los expedientes judiciales o procedimientos administrativos seguidos en forma de juicio que no hayan causado estado.
- Se expone la capacidad de reacción ante posibles ataques informáticos, porque se identificaría o remitiría información contenida en los equipos, servidores, equipos de comunicación, atentando la seguridad y conectividad tecnológica que se tiene implementada.
- La información requerida, en su conjunto, permite que cualquier persona capacitada ingrese a los sistemas de comunicación y a la información que se aloje en esos sistemas.
- La afectación al Alto Tribunal también pone en riesgo la seguridad pública de los justiciables, porque la red de comunicaciones de la Suprema Corte de Justicia de la Nación interconecta con los demás órganos del Poder Judicial de la Federación (Consejo de la Judicatura Federal, Juzgados de Distrito, Tribunales Unitarios, Tribunales Colegiados y Tribunal Electoral del Poder Judicial de la Federación).

De lo anterior se desprende que la información requerida se clasifica como **reservada**, de conformidad con el artículo 113, fracción I de la Ley General de Transparencia, en virtud de que se pondrían en riesgo cuestiones de seguridad y conectividad, lo que derivaría en un posible riesgo para la conducción de expedientes judiciales o de procedimientos administrativos seguidos en forma de juicio.

En ese tenor, debe destacarse que el informe lo emite el área técnica que, conforme a sus atribuciones, es responsable del manejo de los equipos de los que se pide la información y considerando lo resuelto por este Comité en los expedientes CT-CI/A-3-2018, CT-CI/A-5-2018 y CT-CI/A-11-2018, se arriba a la conclusión que sobre la información requerida sí pesa la reserva establecida en la fracción I, del artículo 113, de la Ley General de Transparencia que establece:

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

En efecto, acorde con lo resuelto por este Comité en los asuntos listados, se actualiza esa hipótesis, porque se podría comprometer un aspecto de la seguridad pública en general, ya que el área técnica mencionó que, en general, se pondría en riesgo la información contenida en los equipos de cómputo y con ello se potencializaría el nivel vulnerabilidad ante posibles ataques informáticos y suplantación de identidad.

Para explicar esa conclusión, debe tenerse en cuenta que de conformidad con lo dispuesto en los artículos 100, último párrafo de la Ley General[3], en relación con el 17, párrafo primero Acuerdo General de

[3] ***"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."

Administración 5/2015[4], es competencia del titular de la instancia que tiene bajo su resguardo la información requerida, determinar su disponibilidad y clasificarla conforme a los criterios establecidos en la normativa aplicable.

Así, conforme a lo anterior, se tiene que la Dirección General de Tecnologías de la Información es la única área técnica que cuenta con el personal especializado para velar por la seguridad de la información contenida en los sistemas tecnológicos del Alto Tribunal.

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

De manera similar a lo argumentado, en la resolución CT-CI/A-3-2018, este Comité de Transparencia identifica que se pretende proteger, desde un esquema global, los equipos de cómputo y la información relacionada con aspectos vinculados con la seguridad técnica de los sistemas tecnológicos del Alto Tribunal, en tanto que se podrían involucrar negativamente aspectos de seguridad pública que inciden directamente en su tarea sustantiva, ya que se podría acceder a la información inmersa en dichos equipos y con ello, se reitera, potencializar el nivel de vulnerabilidad de un ataque informático y suplantación de identidad para acceder a la infraestructura tecnológica no sólo de esta Suprema Corte de Justicia de la

---

[4] ***"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…"

Nación sino también de los demás órganos del Poder Judicial de la Federación.

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

Lo anterior, porque se podrían poner en riesgo cuestiones de seguridad pública, ya que, según se refirió previamente, a partir del uso del número de serie sería posible dar o remitir a diversa información que permita identificar las tecnologías, esquemas de conectividad y de seguridad, así como equipos y tecnologías que se emplean en el Alto Tribunal, facilitando ataques cibernéticos.

En ese orden de ideas, lo que se impone es **clasificar** como reservada la información solicitada, con fundamento en la fracción I del artículo 113 de la Ley General de Transparencia, por un plazo de cinco años, atendiendo a lo establecido en el artículo 101[5], de la Ley General de Transparencia.

---

[5] ***"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.

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."

Lo anterior no implica una limitación al derecho de acceso a la información, en tanto que el conocimiento relacionado con los equipos de cómputo de este Alto Tribunal, así como cualquier otro tipo de bienes tecnológicos, puede ser objeto de escrutinio público, es decir, puede obtenerse información de diversas maneras, sin la necesidad de que se proporcionen elementos que lleven a identificar sistemas de comunicaciones tecnológicos que pongan en riesgo la información contenida en dichos equipos o sistemas como ocurre en este caso[6].

Por lo expuesto y fundado; se,

R E S U E L V E:

ÚNICO. Se confirma la clasificación de reserva temporal de la información solicitada, acorde con lo señalado en esta resolución.

Notifíquese a la persona 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 la maestra Fabiana Estrada Tena, Secretaria Jurídica de la Presidencia y Presidenta del Comité, Magistrado Constancio Carrasco Daza, titular de la Unidad General de Enlace con los Poderes Federales, y licenciado Juan Claudio Delgado Ortiz Mena, Contralor del Alto Tribunal; quienes firman con el secretario del Comité que autoriza.

---

[6] *Para tal efecto puede consultarse la Plataforma Nacional de Transparencia, en la siguiente liga: http://consultapublicamx.inai.org.mx:8080/vut-web/*
Llenar los campos de: Entidad Federativa con Federación"; Sujeto Obligado con "Suprema Corte de Justicia de la Nación"; Ley con "Ley General de Transparencia y Acceso a la Información Pública_Ámbito Federal"; Artículo con "Art. 70- En la Ley Federal y de las Entidades federativas se contemplará que los sujetos obligados pongan a disposición del…" y "XXXIV – Inventario de bienes muebles".

MAESTRA FABIANA ESTRADA TENA
PRESIDENTA DEL COMITÉ

MAGISTRADO CONSTANCIO CARRASCO DAZA
INTEGRANTE DEL COMITÉ

LICENCIADO JUAN CLAUDIO DELGADO ORTIZ MENA
INTEGRANTE DEL COMITÉ

LICENCIADO CARLOS GUSTAVO PONCE NÚÑEZ
SECRETARIO DEL COMITÉ