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

CUMPLIMIENTO CT-CUM/A-2-2024
Derivado del expediente CT-CI/A-1-2019

INSTANCIA VINCULADA:

DIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN

Ciudad de México. Resolución del Comité de Transparencia de la Suprema Corte de Justicia de la Nación, correspondiente al veinticuatro de enero de dos mil veinticuatro.

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

PRIMERO. 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*

CSmO+S2c1cvoDCcPk+wkIX27X4wwQpDSB9XHbAX1U58=

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."*

SEGUNDO. Resolución del Comité de Transparencia en la que se clasificó información. En sesión de treinta de enero de dos mil diecinueve, este Comité de Transparencia emitió resolución en el expediente CT-CI/A-1/2019[1], conforme se transcribe en lo conducente:

> ***"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.*
>
> *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.*

[1] Disponible en: https://www.scjn.gob.mx/sites/default/files/resoluciones/2019-02/CT-CI-A-1-2019.pdf

CSmO+S2c1cv0DCcPk+wkIX27X4wwQpDSB9XHbAX1U58=

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 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.*
- *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

CSmO+S2c1cv0DCcPk+wkIX27X4wwQpDSB9XHbAX1U58=

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, en relación con el 17, párrafo primero Acuerdo General de Administración 5/2015, 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 (sic) *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 Nación sino también de los demás órganos del Poder Judicial de la Federación.

CSmO+S2c1cv0DCcPk+wkIX27X4wwQpDSB9XHbAX1U58=

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, de la Ley General de Transparencia.*

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.

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.”*

TERCERO. **Requerimiento para actualizar el índice de información reservada.** Mediante oficio CT-2-2024, enviado por correo electrónico el dos de enero de dos mil veinticuatro, la Secretaría Técnica de este Comité de Transparencia solicitó a la Dirección General de Tecnologías de la Información (DGTI), que se pronunciara sobre la vigencia de la reserva de la información clasificada en la resolución antes transcrita, o bien, si procedía su desclasificación.

CSmO+S2c1cvoDCcPk+wkIX27X4wwQpDSB9XHbAX1U58=

CUARTO. Informe de la DGTI sobre el seguimiento al índice de información reservada. El nueve de enero de dos mil veinticuatro, se remitió por el Sistema de Gestión Documental Institucional, el oficio DGTI/18/2024, con el que el titular de la DGTI remite la Atenta Nota de Cumplimiento números DGTI/SGST-01-2024 y DGTI/DSI-01-2024, del Subdirector General de Servicios Tecnológicos, el Director de Cómputo Personal, el Director de Seguridad Informática y el Subdirector de Ciberseguridad, en la que se informa:

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

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

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

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

> *'Para la aplicación de la prueba de daño a la que hace referencia el artículo 104 de la Ley General de Transparencia y Acceso a la Información Pública, los sujetos obligados atenderán lo siguiente:*
> *I. Se debe citar la fracción y, en su caso, la causal aplicable del artículo 113 de la Ley General de Transparencia y Acceso a la Información Pública, vinculándola con*

CSmO+S2c1cvoDCcPk+wkIX27X4wwQpDSB9XHbAX1U58=

el Lineamiento específico y, cuando corresponda, el supuesto normativo que expresamente le otorga el carácter de información reservada.
II. Mediante la ponderación de los intereses en conflicto, los sujetos obligados deben demostrar que la publicidad de la información solicitada generaría un riesgo de perjuicio y por lo tanto, tendrán que acreditar que este último rebasa el interés público protegido por la reserva.
III. Se debe de acreditar el vínculo entre la difusión de la información y la afectación del interés jurídico tutelado de que se trate.
IV. Precisar las razones objetivas por las que la apertura de la información generaría una afectación, a través de los elementos de un riesgo real, demostrable e identificable.
V. En la motivación de la clasificación, el sujeto obligado deberá acreditar las circunstancias de modo, tiempo y lugar del daño.
VI. Deberán elegir la opción de excepción al acceso a la información que menos lo restrinja, la cual será adecuada y proporcional para la protección del interés público, y deberá interferir lo menos posible en el ejercicio efectivo del derecho de acceso a la información.'

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

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

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

- *Existe un riesgo real, demostrable e identificable de perjuicio significativo al interés público, toda vez que la difusión de lo requerido revelaría información sobre la infraestructura y seguridad tecnológica del Alto Tribunal, lo que implicaría para la Suprema Corte de Justicia de la Nación a un estado de vulnerabilidad, ya que podría poner en riesgo cuestiones de seguridad pública y, con ello, el acceso a la justicia.*
- *Se supera el interés público general de conocer la información, porque existe un interés público superior de proteger la seguridad pública en general, ya que el daño que podría producirse con la publicidad de la información es mayor que el interés de conocerla; toda vez que al divulgar la información referente a número de serie de equipos de cómputo, así como los sistemas operativos, nombres comerciales, versiones y vigencias de los antivirus o software de seguridad en Internet instalados en éstos, lista de las páginas web*

CSmO+S2c1cv0DCcPk+wkIX27X4wwQpDSB9XHbAX1U58=

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, se podrían presentar las siguientes consecuencias:

- ✓ *Ataques a la Suprema Corte consistentes en la 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 de la Institución 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 de esta Suprema Corte 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 Poder Judicial de la Federación (PJF), constituyendo una cuestión de seguridad pública tanto para el PJF, como para los justiciables; ya que la red de comunicaciones de la Suprema Corte, interconecta con los demás órganos del PJF, esto es, con el Consejo de la Judicatura Federal (CJF), Juzgados de Distrito, Tribunales Unitarios, Tribunales Colegidos y el Tribunal Electoral del PJF.*

- ✓ *El proteger la información clasificada como reservada se adecua al principio de proporcionalidad, en tanto que se justifica negar su divulgación por el riesgo a afectar la capacidad de reacción de la Suprema Corte ante posibles ataques informáticos, así como generar un alto riesgo de suplantación de identidad del equipo para acceder a la red y a toda la infraestructura tecnológica y de comunicaciones, lo cual permitiría extraer la información contenida en los equipos de este Alto Tribunal, poniendo en riesgo cuestiones de seguridad pública y, con ello, el acceso a la justicia. Ello, aunado a que la clasificación como reservada de la información, constituye el medio menos lesivo para la adecuada tutela del bien jurídico tutelado como es la seguridad pública general.*

CSmO+S2c1cv0DCcPk+wkIX27X4wwQpDSB9XHbAX1U58=

Todo lo anteriormente expuesto, se refuerza con lo resuelto por el propio Comité de Transparencia de la Suprema Corte de Justicia de la Nación, a través de la resolución del expediente de cumplimiento CT-CI/A-1-2019, (sic) *el cual señala lo siguiente:*

> *'…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 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 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.*
> - *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).*

CSmO+S2c1cv0DCcPk+wkIX27X4wwQpDSB9XHbAX1U58=

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 CTCI/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:*

General de Transparencia (sic) *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.

…

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 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, de la Ley General de Transparencia.

Así como lo señalado por la resolución dentro del expediente de cumplimiento CT-CUM/A-20-2023 derivado del expediente CT-CI/A-11-2018, de fecha veintiuno de junio de dos mil veintitrés, la cual señala:

CSmO+S2c1cv0DCcPk+wkIX27X4wwQpDSB9XHbAX1U58=

En seguimiento a la solicitud, mediante resolución CT-CI/A-11-2018 este órgano colegiado determinó clasificar como reservada la información solicitada, por actualizarse el supuesto del artículo 113, fracción I, de la Ley General de Transparencia.

Lo anterior, partiendo de lo determinado por este órgano colegiado en el expediente CT-CI/A-5-201811 (sic) *en el cual se validó que la documentación relacionada con la tecnología, su ubicación, números de serie, marca, contraseñas, sitios, esquemas de conectividad y de seguridad, así como equipos que se usan para salvaguardar la información del sistema de comunicaciones de este Alto Tribunal es de carácter reservado, por lo cual* ***el veintisiete de junio de dos mil dieciocho en el expediente CT-CI/A-11-2018 éste Comité resolvió confirmar la clasificación hecha por el área vinculada en relación con la información solicitada en el caso, al haberse actualizado el supuesto del artículo 113, fracción I, de la Ley General de Transparencia con la tecnología, su ubicación, números de serie, marca, contraseñas, sitios, esquemas de conectividad y de seguridad****, así como equipos que se usan para salvaguardar la información del sistema de comunicaciones de este Alto Tribunal es de carácter reservado, por lo cual el veintisiete de junio de dos mil dieciocho en el expediente CT-CI/A-11-2018* ***éste Comité resolvió confirmar la clasificación hecha por el área vinculada en relación con la información solicitada en el caso, al haberse actualizado el supuesto del artículo 113, fracción I, de la Ley General de Transparencia.***

Lo que antecede, porque ***en esencia se estableció que con la divulgación de la información solicitada se podrían identificar las tecnologías, esquemas de conectividad y de seguridad, que se emplean en este Alto Tribunal para salvaguardar la información contenida en los sistemas de comunicaciones, lo cual pondría en riesgo cuestiones de seguridad pública.***

A partir de lo anterior, en la mencionada resolución se estableció el plazo de reserva de cinco años, atento a lo establecido en el artículo 101 de la Ley General de Transparencia.

Derivado de los recursos de revisión interpuestos por la persona denunciante en contra de la referida clasificación, el Pleno del INAI en resolución de treinta y uno de octubre de dos mil dieciocho dictada en el expediente RRA 6064/18 que acumuló al 6063/18, determinó lo siguiente:

- *Número de serie, de cada uno de los equipos de cómputo, y de cada uno de los MODEMS, ROUTERS o puntos de acceso inalámbricos, en posesión del sujeto obligado.*

- *Una relación de todos los puertos de red abiertos.*

- *El nombre y versión del programa informático instalado para administrar o controlar lo referente al cortafuegos o firewall.*

- *Si se encuentra habilitada la conexión de red IPv6 (Protocolo de Internet versión 6).*

- *Nombre de las personas físicas que cuentan con las contraseñas administrativas o su equivalente (permisos informáticos, credenciales administrativas, privilegios de superusuario)* [sic] *para el manejo, administración y control de la configuración de cada equipo.*

- *La forma en que cada equipo obtiene o asigna, según sea el caso, la dirección IP (por sus siglas en inglés Internet protocol) privada en la red (de forma manual o por medio del Protocolo de Configuración Dinámica de Host.*

- *El domicilio actual en donde se encuentra físicamente cada equipo.*

CSmO+S2c1cv0DCcPk+wkIX27X4wwQpDSB9XHbAX1U58=

Lo anterior ***por considerar que la divulgación de la información constituye un riesgo real, demostrable e identificable de perjuicio significativo al interés público, ya que se podría obstaculizar o bloquear las actividades de inteligencia o contrainteligencia y revelarse normas, procedimientos, métodos, fuentes, especificaciones técnicas, tecnología o equipo que sean útiles para la generación de inteligencia para la seguridad nacional****.*

Ahora, ya que el plazo de reserva de la información está próximo a concluir, la Secretaría de este órgano colegiado solicitó a la Dirección General de Tecnologías de la Información que emitiera un informe en el que señalara si prevalecía la reserva temporal de la información o si procedía su desclasificación.

En respuesta a ello, ***la instancia vinculada informó que subsisten las causas que dieron origen a su clasificación de conformidad con lo dispuesto en el artículo 113, fracción I,*** *de la Ley General de Transparencia y Acceso a la Información Pública, en el caso existe un riesgo real, demostrable e identificable de perjuicio significativo al interés público.*

En el caso, la citada Dirección General señala que en términos del artículo 113, fracción I, de la Ley General de transparencia, persisten las causas que dieron origen a la clasificación de la información solicitada, por las razones siguientes:

a) Existe un riesgo real, demostrable e identificable de perjuicio significativo al interés público, ***ya que, con la divulgación de lo requerido, se pudieran revelar especificaciones técnicas, de los equipos, conexiones y programas que pudieran vulnerar la seguridad pública al haber riesgo en la intromisión no permitida****.*

b) Se supera el interés público general de conocer la información porque ***existe un interés público superior de proteger la seguridad pública en general****, porque el daño que podría producirse con la publicidad de la es mayor que el interés de conocerla; toda vez que al divulgar la información se podrían presentar las siguientes consecuencias:*

- *La* ***suplantación de identidad*** *para acceder a la red y a toda la infraestructura tecnológica y de comunicaciones de este Alto Tribunal****, con lo que podría extraerse información sobre las actividades de esta Suprema Corte de Justicia de la Nación****.*

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

- ***Se pondrían en riesgo otras instancias del Poder Judicial de la Federación****, teniendo como una cuestión de seguridad pública tanto para el propio Poder Judicial como para los justiciables, ya que la red de comunicaciones de la Suprema Corte de Justicia de la Nación interconecta con los demás órganos del propio Poder Judicial.*

- ***Se expondría la capacidad de reacción de la Suprema Corte de Justicia de la Nación ante posibles ataques cibernéticos****, además de comprometer un aspecto de la seguridad pública en general.*

El proteger la información clasificada como reservada se adecua al principio de proporcionalidad, en tanto que se justifica negar su divulgación por el riesgo de que se pudieran obstaculizar o bloquear las actividades de este Alto Tribunal accediendo a inteligencia o contrainteligencia y revelarse normas, procedimientos, métodos, fuentes especificaciones técnicas, tecnología o equipo, vulnerando así que sean útiles para la generación de inteligencia para la seguridad nacional. Ello, aunado a que la clasificación como reservada de la información, constituye el medio menos lesivo para la adecuada tutela del bien jurídico tutelado como es la seguridad pública general.

CSmO+S2c1cvoDCcPk+wkIX27X4wwQpDSB9XHbAX1U58=

> ***Como se advierte, los argumentos de la prueba de daño están encaminados a actualizar la causal de reserva prevista en la fracción I del artículo 113 de la Ley General de Transparencia, en tanto que poner a disposición la información en comento comprometería la seguridad nacional*.**
>
> *En consecuencia, de acuerdo con los argumentos expuestos por la Dirección General de Tecnologías de la Información, este Comité de Transparencia determina que subsiste el riesgo real, demostrable e identificable que motivó la clasificación en la resolución CT-CI/A-11-2018, por lo que, conforme los artículos 44, fracción VIII, y 103, de la Ley General de Transparencia, se determina justificado ampliar el plazo de reserva con fundamento en el artículo 113, fracción I, de la Ley General de Transparencia. (sic)*

En conclusión, es procedente ampliar la reserva de la información, ya que subsisten las causas que dieron origen a su clasificación, con fundamento en los artículos 99, tercer párrafo y 110, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública y la fracción I del artículo 113, de la Ley General de Transparencia y Acceso a la Información Pública. En el caso concreto, considerando la aplicación de la prueba de daño antes señalada, se justifica que prevalecen las causas que originaron la reserva y por ello el periodo debe ampliarse hasta por un plazo de cinco años adicionales.”

QUINTO. Acuerdo de turno. Mediante proveído de nueve de enero de dos mil veinticuatro, la Presidencia del Comité de Transparencia de este Alto Tribunal, con fundamento en los artículos 44, fracción VIII, 101, 103 y 27, del Acuerdo General de Administración 5/2015, ordenó integrar el expediente de cumplimiento **CT-CUM/A-2-2024** y remitirlo al Contralor del Alto Tribunal, lo que se hizo mediante oficio CT-05-2024, enviado por correo electrónico en la misma fecha.

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

PRIMERA. Competencia. El Comité de Transparencia de la Suprema Corte de Justicia de la Nación es competente para pronunciarse sobre la ampliación del periodo de reserva de la información, en términos de los artículos 6° de la Constitución Política de los Estados Unidos Mexicanos, 4 y 44, fracción VIII, y 101, párrafo tercero, de la Ley General de Transparencia y Acceso a Información

CSmO+S2c1cvoDCcPk+wkIX27X4wwQpDSB9XHbAX1U58=

Púbica (Ley General de Transparencia), así como 23, fracción I, del Acuerdo General de Administración 5/2015.

SEGUNDA. Análisis. En la solicitud que da origen a este asunto se pidió información sobre cada uno de los equipos de cómputo en posesión de la Suprema Corte de Justicia de la Nación (SCJN), consistente en:

1. A partir del número de serie:
   - Nombres comerciales de los sistemas operativos instalados.
   - Nombres comerciales y versiones de los antivirus o *software* de seguridad de internet.
   - Vigencias de los antivirus o *software* de seguridad instalados.

2. Listas de las páginas webs utilizadas en las páginas electrónicas o webs oficiales, señalando el protocolo que se utiliza y el tipo de seguridad implementado.

3. Las fechas y duración de los ataques de “Denegación de Servicio” o de “Denegación de Servicio Distribuida padecidos”.

En seguimiento a esa solicitud, en la resolución CT-CI/A-1-2019 de treinta de enero de dos mil diecinueve, se determinó que la información era reservada por cinco años, con fundamento en el artículo 113, fracción I, de la Ley General de Transparencia, substancialmente, conforme a lo siguiente:

- 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 que se emplean en el Alto Tribunal, facilitando ataques cibernéticos.

CSmO+S2c1cv0DCcPk+wkIX27X4wwQpDSB9XHbAX1U58=

Se podría comprometer un aspecto de la seguridad pública en general, ya que el área técnica mencionó que 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.

- Lo que se pretende proteger, desde un esquema global, son los equipos de cómputo y la información relacionada con aspectos vinculados con la seguridad técnica de los sistemas tecnológicos de la SCJN, en tanto que se podrían involucrar negativamente aspectos de seguridad pública que incidirían directamente en su tarea sustantiva, ya que se podría acceder a la información contenida en los equipos y potencializar el nivel de vulnerabilidad de un ataque informático y suplantación de identidad para acceder a la infraestructura tecnológica, no sólo de la SCJN sino también de los demás órganos del Poder Judicial de la Federación (PJF).

Debido a que el plazo de reserva de la información estaba próximo a vencer, la DGTI señala que subsisten las causas que dieron origen a la clasificación de la información como reservada, con fundamento en los artículos 110, fracción I, de la Ley Federal de Transparencia y 113, fracción I, de la Ley General de Transparencia y sobre la prueba de daño prevista en el artículo 104[2] de la Ley General de Transparencia, añadió lo siguiente:

a) Existe un riesgo real, demostrable e identificable de perjuicio significativo al interés público, porque la difusión de lo

[2] *"**Artículo 104.** En la aplicación de la prueba de daño, el sujeto obligado deberá justificar que:*
I. La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público o a la seguridad nacional;
II. El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda, y
III. La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio."

CSmO+S2c1cv0DCcPk+wkIX27X4wwQpDSB9XHbAX1U58=

requerido revelaría información sobre la infraestructura y seguridad tecnológica del Alto Tribunal, lo que implicaría para la SCJN un estado de vulnerabilidad, pues pondría en riesgo cuestiones de seguridad pública y, con ello, el acceso a la justicia.

b) El riesgo de perjuicio que supondría la divulgación de la información supera el interés público general de que se difunda, porque se podrían presentar las siguientes consecuencias:

- La 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 expondría la capacidad de reacción de la SCJN 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, permitiría que cualquier persona capacitada ingrese a los sistemas de comunicación de la SCJN y a la información que se aloje en esos sistemas.
- Cualquier afectación a la SCJN también pondría en riesgo a las otras dos instancias del PJF, constituyendo una cuestión de seguridad pública, porque la red de comunicaciones de la SCJN interconecta a los órganos del PJF.

CSmO+S2c1cv0DCcPk+wkIX27X4wwQpDSB9XHbAX1U58=

c) La clasificación constituye el medio menos lesivo para la adecuada tutela del bien jurídico protegido como es la seguridad pública general, porque, reitera, implicaría revelar información sobre la infraestructura y seguridad tecnológica de la SCJN.

Además, en el informe de la instancia vinculada se transcriben argumentos de las resoluciones CT-CI/A-1-2019 y CT-CUM/A-20-2023[3], este último derivado de los expedientes CT-CI/A-11-2018[4] y CT-CUM-R/A-2-2018[5], para sostener la ampliación del plazo de reserva.

Para realizar el análisis correspondiente, se tiene en cuenta que conforme a los artículos 100[6] de la Ley General de Transparencia y 97[7] de la Ley Federal de Transparencia, en relación con el diverso 17[8] del

---

[3] Disponible en https://www.supremacorte.gob.mx/sites/default/files/resoluciones/2023-08/CT-CUM-A-20-2023.pdf
[4] Disponible en https://www.scjn.gob.mx/sites/default/files/resoluciones/2018-08/CT-CI-A-11-2018.pdf
[5] Disponible en https://www.scjn.gob.mx/sites/default/files/resoluciones/2019-01/CT-CUM-R-A-2-2018.pdf
[6] *"**Artículo 100.** La clasificación es el proceso mediante el cual el sujeto obligado determina que la información en su poder actualiza alguno de los supuestos de reserva o confidencialidad, de conformidad con lo dispuesto en el presente Título.*
Los supuestos de reserva o confidencialidad previstos en las leyes deberán ser acordes con las bases, principios y disposiciones establecidos en esta Ley y, en ningún caso, podrán contravenirla.
Los titulares de las Áreas de los sujetos obligados serán los responsables de clasificar la información, de conformidad con lo dispuesto en esta Ley, la Ley Federal y de las Entidades Federativas."
[7] "***Artículo 97.** La clasificación es el proceso mediante el cual el sujeto obligado determina que la información en su poder actualiza alguno de los supuestos de reserva o confidencialidad, de conformidad con lo dispuesto en el presente Título.*
En el proceso de clasificación de la información, los sujetos obligados observarán, además de lo establecido en el Título Sexto de la Ley General, las disposiciones de la presente Ley.
Los titulares de las Áreas de los sujetos obligados serán los responsables de clasificar la información, de conformidad con lo dispuesto en la Ley General y la presente Ley.
Los sujetos obligados deberán aplicar, de manera restrictiva y limitada, las excepciones al derecho de acceso a la información previstas en el presente Título y deberán acreditar su procedencia, sin ampliar las excepciones o supuestos de reserva o confidencialidad previstos en las leyes, de conformidad con lo establecido en la Ley General.
Los sujetos obligados no podrán emitir acuerdos de carácter general ni particular que clasifiquen documentos o expedientes como reservados, ni clasificar documentos antes de dar respuesta a una solicitud de acceso a la información.
La clasificación de información reservada se realizará conforme a un análisis caso por caso, mediante la aplicación de la prueba de daño."
[8] ***"Artículo 17***
De la responsabilidad de los titulares y los enlaces
En su ámbito de atribuciones, los titulares de las instancias serán responsables de la gestión de las solicitudes, así como de la veracidad y confiabilidad de la información.
A efecto de instituir un vínculo de comunicación para las gestiones derivadas de trámites de acceso a la información, protección de información reservada y/o confidencial y transparencia, los titulares de las instancias designarán un servidor público que fungirá como Enlace e informarán por escrito sobre su designación a la Unidad General."

CSmO+S2c1cvoDCcPk+wkIX27X4wwQpDSB9XHbAX1U58=

Acuerdo General de Administración 5/2015, las personas titulares de las instancias que tienen bajo resguardo la información solicitada son las responsables de determinar su disponibilidad y clasificarla conforme a la normativa aplicable.

En ese sentido, destaca que en términos del artículo 36, fracciones I, V, VI y IX[9], del Reglamento Orgánico en Materia de Administración de la SCJN, la DGTI es el área técnica que cuenta con el personal especializado para velar por la seguridad de los sistemas tecnológicos de este Alto Tribunal, pues le corresponde administrar sus sistemas informáticos jurídicos, administrativos y jurisdiccionales.

La DGTI ha informado que en términos del artículo 113, fracción I, de la Ley General de Transparencia, subsiste el riesgo real, demostrable e identificable que originó que se reservará la información requerida en la solicitud de origen, relativa al número de serie de equipos de cómputo, vinculado con los sistemas operativos, nombres comerciales, versiones y vigencias de los antivirus o software de seguridad en Internet instalados en dichos equipos; 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”.

CSmO+S2c1cvoDCcPk+wkIX27X4wwQpDSB9XHbAX1U58=

---

[9] *“**Artículo 36.** La Dirección General de Tecnologías de la Información tendrá las atribuciones siguientes:*
I. Administrar los recursos en materia de tecnologías de la información y comunicación, así como proveer los servicios que se requieran en la materia;
II. Recabar las necesidades de bienes y servicios en materia de tecnologías de la información y comunicación
(…)
V. Planificar, diseñar, desarrollar y mantener en operación los sistemas informáticos jurídicos, administrativos y jurisdiccionales, así como los portales y micrositios que requieran los órganos y áreas, de conformidad con las disposiciones jurídicas aplicables;
VI. Elaborar estudios técnicos en materia de infraestructura tecnológica, así como de sistemas y bienes informáticos;
(…)
IX. Instrumentar los mecanismos en materia de seguridad informática y vigilar su adecuado funcionamiento;
(…)

Ahora bien, respecto de la información materia de la solicitud de acceso de origen, se tiene que en la resolución CT-CI/A-1-2019 se clasificó como reservada con fundamento en el artículo 113, fracción I, de la Ley General de Transparencia, hipótesis que la instancia responsable señala que subsiste y, por ello, solicita la ampliación del plazo de reserva; sin embargo, este Comité de Transparencia, que actúa con plenitud de jurisdicción, considera que, conforme al artículo 103[10] de la Ley General de Transparencia, a partir de una nueva reflexión, como se hizo al resolver el expediente CT-CUM/A-52-2023[11], además de considerar los argumentos expuestos al resolver los expedientes CT-CI/A-16-2023[12], CT-VT/A-29-2023[13], CT-VT/A-22-2023[14], y la resolución del recurso de revisión 10276/18 del INAI, de la que derivó el cumplimiento CT-CUM-R/A-2-2019[15], se determina que se actualiza la causal de reserva prevista en los artículos 113, fracción VII[16], de la Ley General de Transparencia y 110, fracción VII, de la Ley Federal de Transparencia y no en la fracción I de ambos preceptos.

En ese sentido, se tiene en consideración que la divulgación de la información solicitada podría afectar la capacidad de reacción de la SCJN ante posibles **ataques informáticos**, además de generar un alto riesgo de suplantación de identidad del equipo para acceder a la red y a toda la infraestructura tecnológica y de comunicaciones, lo que

CSmO+S2c1cvoDCcPk+wkIX27X4wwQpDSB9XHbAX1U58=

---

[10] *"Artículo 103. En los casos en que se niegue el acceso a la información, por actualizarse alguno de los supuestos de clasificación, el Comité de Transparencia deberá confirmar, modificar o revocar la decisión.*
Para motivar la clasificación de la información y la ampliación del plazo de reserva, se deberán señalar las razones, motivos o circunstancias especiales que llevaron al sujeto obligado a concluir que el caso particular se ajusta al supuesto previsto por la norma legal invocada como fundamento. Además, el sujeto obligado deberá, en todo momento, aplicar una prueba de daño.
Tratándose de aquella información que actualice los supuestos de clasificación, deberá señalarse el plazo al que estará sujeto la reserva."

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

[12] Disponible en https://www.scjn.gob.mx/sites/default/files/resoluciones/2023-08/CT-CI-A-16-2023.pdf

[13] Disponible en https://www.scjn.gob.mx/sites/default/files/resoluciones/2023-08/CT-VT-A-29-2023.pdf

[14] Disponible en https://www.scjn.gob.mx/sites/default/files/resoluciones/2023-06/CT-VT-A-22-2023.pdf

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

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

permitiría extraer información contenida en los equipos de este Alto Tribunal, poniendo en riesgo cuestiones de seguridad pública y, con ello, el acceso a la justicia; incluso, se pondría en riesgo a las otras instancias del PJF, constituyendo una cuestión de seguridad pública tanto para el PJF, como para los justiciables, porque la red de comunicaciones de la SCJN interconecta con los demás órganos del PJF.

La información requerida constituye información susceptible de mantenerse clasificada como reservada, en tanto que la instancia vinculada informa que se refiere a aspectos relacionados con la infraestructura tecnológica de la SCJN, incluso, que el acceso a dicha información en su conjunto permitiría que cualquier persona capacitada ingrese a los sistemas de comunicación de la SCJN y a la información que se aloje en esos sistemas.

Además, la DGTI, al realizar la prueba de daño, argumentó que existe un riesgo real, demostrable e identificable de perjuicio significativo al interés público, porque la difusión de lo solicitado conllevaría a este Alto Tribunal a un estado de **vulnerabilidad**, en tanto se pondría en riesgo la red y la infraestructura tecnológica y de comunicaciones de la SCJN, así como los equipos de cómputo, servidores y equipos de comunicación.

En consecuencia, se estima que las razones convergen en la actualización de la causal de reserva prevista en la fracción VII del artículo 113 de la Ley General de Transparencia, de cuyo contenido se desprende que se podrá clasificar como información reservada aquella cuya publicación obstruya la prevención o persecución de los delitos.

CSmO+S2c1cv0DCcPk+wkIX27X4wwQpDSB9XHbAX1U58=

Como apoyo a tal conclusión se retoma, en lo que interesa, lo que el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) sostuvo al resolver el recurso de revisión 10276/18[17]:

> (…)
> *"Por todo lo anterior, se advierte que difundir información relativa a los números de serie de los equipos y la versión del firewall instalado,* ***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 esa tónica, 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; resultando, por lo tanto, es procedente su reserva, de conformidad con el precepto jurídico que se analiza.*
>
> *Es decir, este Organismo Garante del derecho de acceso a la información pública concluye que* ***procede la reserva*** *de la información relativa al número de serie, el conocer si los discos duros se encuentran encriptados, el nombre comercial de los programas de encriptado de información, conocer si pueden borrar o no archivos con o sin contraseñas y conocer si se puede almacenar información a través de los puertos USB, de cada uno de los equipos de cómputo en posesión del sujeto obligado, de conformidad con lo previsto en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública."*
> (…)

Conforme a lo expuesto, este Comité concluye que las razones con base en las cuales el INAI determinó que se actualizaba la fracción VII, del artículo 110, de la Ley Federal de Transparencia[18], de contenido

[17] Recurso interpuesto en contra de la clasificación de información CT-CI/A-27-2018, consultable en http://consultas.ifai.org.mx/Sesiones

[18] *"**Artículo 110.** Como información reservada podrá clasificarse aquella cuya publicación:*
(…)

CSmO+S2c1cvoDCcPk+wkIX27X4wwQpDSB9XHbAX1U58=

idéntico al artículo 113, fracción VII, de la Ley General de Transparencia, son coincidentes con las expuestas por la instancia vinculada para motivar la ampliación del plazo de reserva de la información que dio origen a este asunto, en virtud de que confluyen en la posibilidad de una **vulneración a la seguridad de la infraestructura tecnológica de este Alto Tribunal**, así como en facilitar la extracción, modificación o alteración de información relevante.

Por cuanto hace a la prueba de daño y en concordancia con los argumentos señalados, se estima que subsisten las causas que dieron origen a la clasificación de la información relativa al número de serie de los equipos, vinculado con 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".

Al respecto, se retoma lo señalado por este Comité al resolver el expediente CT-CUMR/A-2-2019[19]: *"como información reservada podrá clasificarse aquella cuya publicación obstruya la prevención o persecución de delitos"*, a lo que se agrega 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"* y que *"para que pueda acreditarse que la información requerida pudiera 'obstruir la prevención de los delitos',*

VII. *Obstruya la prevención o persecución de los delitos;"*
(…)
[19] En cumplimiento del recurso de revisión 10276/18 del INAI.

CSmO+S2c1cv0DCcPk+wkIX27X4wwQpDSB9XHbAX1U58=

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”.

También es aplicable en el caso que nos ocupa, lo argumentado en dicha resolución, acerca de 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 (…) *“‘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”*.

Además, se hizo alusión al Código Penal Federal en los términos siguientes: *“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”.*

CSmO+S2c1cv0DCcPk+wkIX27X4wwQpDSB9XHbAX1U58=

Por consiguiente, en términos del artículo 104 de la Ley General de Transparencia, se concluye que el daño que podría producirse con la publicidad de la información materia de la solicitud de origen es mayor que el interés de conocerla, pues como se argumentó, la difusión de lo solicitado podría afectar la capacidad de reacción de la SCJN ante posibles ataques informáticos, así como generar un alto riesgo de suplantación de identidad del equipo para acceder a la red y a toda la infraestructura tecnológica y de comunicaciones, lo que permitiría extraer la información contenida en los equipos de este Alto Tribunal, poniendo en riesgo cuestiones de seguridad pública y, con ello, el acceso a la justicia, lo que incidiría directa y negativamente en la tarea sustantiva de la SCJN; además, se podría comprometer la información de los demás órganos del PJF.

En ese orden de ideas, de conformidad con los artículos 44, fracción VIII, y 103, de la Ley General de Transparencia, se determina justificado ampliar el plazo de reserva respecto de la información materia de la solicitud de acceso que da origen a este asunto con fundamento en el artículo 113, fracción VII, de la Ley General de Transparencia.

Respecto del plazo de reserva, se tiene en cuenta que el artículo 101 de la Ley General de Transparencia contempla la posibilidad de que pueda ampliarse hasta por cinco años adicionales, cuando se justifique que prevalecen las causas que dieron origen a su clasificación, lo que ha quedado demostrado en este caso; por tanto, la ampliación que se autoriza es de cinco años más que se computarán a partir del vencimiento del primer periodo de reserva, en el entendido de que podrá concluir previamente, siempre que se extingan las causas de clasificación.

CSmO+S2c1cv0DCcPk+wkIX27X4wwQpDSB9XHbAX1U58=

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, en los términos expuestos en la presente resolución.

Notifíquese 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 licenciado Mario José Pereira Meléndez, Director General de Asuntos Jurídicos y Presidente del Comité, maestro Christian Heberto Cymet López Suárez, Contralor del Alto Tribunal, y licenciado Adrián González Utusástegui, Titular de la Unidad General de Investigación de Responsabilidades Administrativas; quienes firman con la secretaria del Comité que autoriza.

LICENCIADO MARIO JOSÉ PEREIRA MELÉNDEZ
PRESIDENTE DEL COMITÉ

MAESTRO CHRISTIAN HEBERTO CYMET LÓPEZ SUÁREZ
INTEGRANTE DEL COMITÉ

LICENCIADO ADRIÁN GONZÁLEZ UTUSÁSTEGUI
INTEGRANTE DEL COMITÉ

CSmO+S2c1cvoDCcPk+wkIX27X4wwQpDSB9XHbAX1U58=

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."

CSmO+S2c1cv0DCcPk+wkIX27X4wwQpDSB9XHbAX1U58=