CLASIFICACIÓN DE INFORMACIÓN CT-CI/A-27-2018

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 y uno de octubre de dos mil dieciocho.

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

I. Solicitud de información. El veinticuatro de septiembre de dos mil dieciocho, se recibió en la Plataforma Nacional de Transparencia la solicitud tramitada con el folio 0330000178918, 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 aplicables.*
>
> 1. *Por número de serie de cada uno de los equipos de cómputo en posesión del sujeto obligado requiero.*
>
>   a) *Si actualmente los archivos electrónicos almacenados en la unidad de disco duro (que no sean del sistema operativo) cuentan con algún tipo de cifrado, cuyo control se efectué por medio de contraseñas o credenciales administrativas.*
>   b) *Nombres comerciales de los programas informáticos utilizados para el cifrado de los archivos mencionados en el inciso anterior.*
>   c) *Si actualmente los usuarios del equipo pueden borrar los archivos electrónicos almacenados en la unidad de disco duro (que no sean del sistema operativo), sin la necesidad de contar con privilegios o contraseñas administrativas.*
>   d) *Si se encuentra instalado el navegador de Internet denominado Tor Browser.*
>   e) *Número de puertos USB (por siglas en ingles Universal Serial Bus) habilitado para su funcionamiento.*
>   f) *Si actualmente los usuarios del equipo pueden copiar los archivos almacenados en la unidad de disco duro (que no sean del sistema operativo) a través de los puertos USB mencionados en el punto anterior, sin la necesidad de contar con privilegios o contraseñas administrativas."*

“Otros datos para facilitar su localización
QUINTO TRIBUNAL COLEGIADO DE CIRCUITO EN MATERIA PENAL CDMX”

II. Prevención. En proveído de veintiséis de septiembre de dos mil dieciocho, por conducto del Subdirector General de la Unidad General de Transparencia y Sistematización de la Información Judicial, con fundamento en los artículos 128 y 129 de la Ley General de Transparencia y Acceso a la Información Pública, 129 de la Ley Federal de Transparencia y Acceso a la Información Pública y 8 del Acuerdo General de Administración 5/2015, se previno al solicitante para que precisara *“si la información solicitada es del ‘Quinto Tribunal Colegiado de Circuito en Materia Penal en la Ciudad de México’”* (foja 5).

III. Desahogo de la prevención. El tres de octubre de este año, el solicitante señaló (fojas 12 y 13):

> *“En atención a su requerimiento preciso que en función de los principios constitucionales de máxima publicidad, transparencia, rendición de cuentas y gratuidad, la información pública solicitada es la siguiente: 1. Por número de serie de cada uno de los equipos de cómputo en posesión del sujeto obligado requiero: a) Si actualmente los archivos electrónicos almacenados en la unidad de disco duro (que no sean del sistema operativo) cuentan con algún tipo de cifrado, cuyo control se efectué por medio de contraseñas o credenciales administrativas. b) Nombres comerciales de los programas informáticos utilizados para el cifrado de los archivos mencionados en el inciso anterior. c) Si actualmente los usuarios del equipo pueden borrar los archivos electrónicos almacenados en la unidad de disco duro (que no sean del sistema operativo), sin la necesidad de contar con privilegios o contraseñas administrativas. d) Si se encuentra instalado el navegador de Internet denominado Tor Browser. e) Número de puertos USB (por sus siglas en ingles Universal Serial Bus) habilitados para su funcionamiento. f) Si actualmente los usuarios del equipo pueden copiar los archivos almacenados en la unidad de disco duro (que no sean del sistema operativo) a través de los puertos USB mencionados en el punto anterior, sin la necesidad de contar con privilegios o contraseñas administrativas.*
>
> *NOTA: Se reitera me entregue la información 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,”*

IV. Admisión de la solicitud. Desahogada la prevención, por conducto del Subdirector General de la Unidad General de Transparencia, 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, en acuerdo de cuatro de octubre de este año, se estimó procedente la solicitud y se ordenó abrir el expediente UT-J/0382/2018 (fojas 14 y 15).

V. Requerimiento de información. Por oficio UGTSIJ/TAIPDP/2687/2018, el nueve de octubre 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 16).

VI. Respuesta de la Dirección General de Tecnologías de la Información. El dieciocho de octubre de dos mil dieciocho, se recibió en la Unidad General de Transparencia el oficio DGTI/DAPTI-2223-2018, en el que se informa lo siguiente:

> *"Respuesta:*
>
> *Del análisis a la solicitud, se desprende que el solicitante requiere que a partir del número de serie se le proporcione diversa información relacionada a las medidas de seguridad de los equipos de cómputo de este Alto Tribunal. Para ello, se hace referencia a lo previamente resuelto por el Comité de Transparencia en su Octava Sesión Pública Ordinaria celebrada el dieciocho de abril del año en curso relacionada al expediente de Clasificación de información CT-CI/A-3-2018, en el que acordaron clasificar como reservado el número de serie, con base en la fracción I, del artículo 113 de la Ley General, por un plazo de cinco años en atención a lo establecido por el artículo 1014* (sic)*, de la Ley General.*
>
> *Considerando que la información que se solicita está vinculada al ámbito de la seguridad informática, es dable comentar que para garantizar la confidencialidad de un documento electrónico, se hace uso de los denominados 'Algoritmos o métodos de cifrado'; los cuales se encargan de transformar el contenido del documento en un conjunto de caracteres sin orden o significado, con la finalidad de que únicamente la persona que tenga la llave o clave de acceso, pueda tener acceso al equipo y a la información del documento.*
>
> *Para poder realizar el cifrado de un documento se pueden realizar diversos métodos del cifrado, los cuales pueden ir desde un procedimiento sencillo (como puede ser la sustitución o cambio de caracteres dentro del documento) hasta el uso*

de algoritmos científicos y comerciales; los cuales realizan una gran cantidad de procesos de cómputo.

Cuando se da a conocer un método de cifrado, se da a conocer el proceso de cómo fue cifrado el documento, lo que permite que en caso de tratarse de un método obsoleto o de complejidad baja, se pueda llegar a acceder a la información de manera sencilla.

Por otro lado, el método de cifrado de cualquier equipo, como puede ser comunicaciones, equipos de seguridad, cifrado de correo, cifrado de documentos, permite dar a conocer a cualquier individuo la técnica que hacen uso para proteger la información procesada en estos elementos de cómputo, facilitando y dirigiendo un ataque para la obtención de la información.

A continuación, se listan diversos riesgos identificados en los incisos a, b, c, e y f requeridos por el peticionario:

- *El informar que los archivos almacenados en el disco duro cuentan con algún cifrado y que estos son controlados mediante contraseñas, así como el develar que los usuarios no pueden borrar ni copiar archivos en el disco duro sin necesidad de contar con privilegios o contraseñas administrativas; permitiría dar a conocer que para acceder a todos los equipos de este alto tribunal se requieren contraseñas, lo cual pone en riesgo la integridad física de los usuarios en caso de algún robo premeditado o intencional para la extracción de la información; al tratar de obtener las llaves de cifrado para extraer o manipular la información contenida en los equipos, todo esto con base en lo establecido en la fracción V 'Pueda poner en riesgo la vida, seguridad o salud de una persona física' del artículo 113 de la Ley General.*
- *El proporcionar los nombres comerciales de los sistemas informáticos utilizados para el cifrado de archivos, podría permitir a los ciber delincuentes encontrar las llaves para su descifrado en el mercado negro.*
- *Es de resaltar, que los archivos almacenados en los equipos, contienen información relacionados al trabajo diario de los servidores públicos que laboran en esta institución y en el cual puede existir información relacionada con los procesos o asuntos en trámite que tenga el personal según el ámbito de su competencia.*
- *En relación al número de puertos USB habilitados para su funcionamiento, se informa que considerando la norma ISO 27002, estándar internacional para la seguridad de la información, la cual proporciona diferentes recomendaciones de las mejores prácticas en la gestión de la seguridad de la información para iniciar, implementar o mantener sistemas de gestión de la seguridad de la información, el uso de la informática móvil implica considerar los riesgos de trabajar en entornos desprotegidos y aplica la protección conveniente; estableciendo que se deben adoptar las medidas de seguridad adecuadas para la protección contra riesgos derivados del uso de los recursos de informática móvil, entre ellos, los dispositivos USB. Por otra parte, de acuerdo a lo establecido en el Acuerdo General IV/2008 relativo al uso y aprovechamiento de los bienes y servicios informáticos de la SCJN, la Dirección General de Tecnologías de la Información puede restringir el acceso a un recurso, en este caso los puertos USB, considerando las medidas de seguridad aplicables y reservándose la difusión de las medidas de seguridad adoptadas, identificándose que el dar a conocer esta información, también vulnera el acceso a la*

> *información de los equipos y a las personas, ya que mediante estos puertos se puede insertar algún virus, programa informáticos o información maliciosa que perjudique al servidor público y a la institución, si tomamos en cuenta que dicho equipo se conecta a la red de comunicaciones de este alto tribunal, lo cual podría generar suplantación de identidad en la misma.*
>
> *d) Los equipos que proporciona esta Dirección General de forma predeterminada, llevan enlistados los navegadores Microsoft Edge y Microsoft Internet Explorer. El navegador Tor Browser no se encuentra instalado.*
>
> *Conclusión:*
>
> *Como se puede advertir, la información que solicitan está relacionada con la accesibilidad a los equipos de cómputo, cuyos cuestionamientos son específicamente hacia aspectos que tienen que ver con las medidas de seguridad internas; adicional a que solicitan la información detallada del cifrado de los archivos, nombres comerciales de los programas informáticos utilizados para el cifrado, permisos a los usuarios de borrar o copiar sus archivos en los discos duros y puertos USB habilitados en los equipos; todo esto, por cada uno de los equipos en posesión de este alto tribunal mediante el número de serie (clasificado como reservado). El proporcionar esta información, devela el esquema de seguridad que se tiene para cada uno de los equipos de este alto tribunal, lo cual pondría en riesgo tanto al personal como a la institución, dejándonos en un estado de vulnerabilidad muy alto. De lo anterior, se reitera la clasificación de la información como reservada."*

VII. Vista a la Secretaría del Comité de Transparencia. El veintitrés de octubre de dos mil dieciocho, el Titular de la Unidad General de Transparencia y Sistematización de la Información Judicial, a través del oficio UGTSIJ/TAIPDP/2866/2018, remitió el expediente UT-A/0382/2018 a la Secretaría del Comité de Transparencia, con la finalidad de que se dictara la resolución correspondiente.

VIII. Acuerdo de turno. Mediante acuerdo de veinticuatro de octubre de dos mil dieciocho, el Presidente del Comité de Transparencia, 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-27-2018** 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-1616-2018 en esa misma fecha.

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. Materia de análisis. Como se aprecia del antecedente I, en la solicitud se pide que a partir del número de serie de cada uno de los equipos de cómputo en posesión de la Suprema Corte de Justicia de la Nación, se informe lo siguiente:

a) Si los archivos almacenados en el disco duro cuentan con algún tipo de cifrado, cuyo control se efectúe por contraseñas o credenciales administrativas.
b) Nombres comerciales de los programas informáticos utilizados para el cifrado.
c) Si los usuarios de los equipos pueden borrar los archivos almacenados en el disco duro, sin la necesidad de contar con privilegios o contraseñas administrativas.
d) Si se encuentra instalado el navegador de Internet denominado “Tor Browser”.
e) Número de puertos “USB” habilitados para su funcionamiento.
f) Si los usuarios de los equipos pueden copiar los archivos almacenados en el disco duro, a través de los puertos “USB”, sin la necesidad de contar con privilegios o contraseñas administrativas.

Conforme al informe transcrito en el antecedente VI, se tiene por atendido lo requerido en el inciso d), en virtud de que la Dirección General de Tecnologías de la Información informó que los equipos que proporciona de forma predeterminada llevan enlistados los navegadores *"Microsoft Edge y Microsoft Internet Explorer"*, pero el navegador "Tor Browser" no se encuentra listado; por tanto, la Unidad General de Transparencia deberá hacer del conocimiento peticionario dicha respuesta y ello no será materia de análisis en la presente resolución.

III. Análisis. Información reservada.

Por cuanto a lo requerido en los incisos a), b), c), e) y f) de la solicitud, la Dirección General de Tecnologías de la Información informó que la divulgación de esa información podría comprometer, en distintos aspectos, la seguridad informática de este Alto Tribunal, de ahí que clasifica la información como reservada en términos del artículo 113, fracción I de la Ley General de Transparencia y con apoyo en lo resuelto por este Comité en el expediente CT-CI/A-3-2018.

Sobre esa base, el punto a dilucidar a través del caso que nos ocupa radica en si sobre la información solicitada se actualiza o no la reserva identificada por la instancia requerida y, en su caso, si aquella puede o no ser proporcionada en los términos solicitados.

Antes de llevar a cabo el análisis correspondiente, es importante recordar 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, 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.

Trasladado al caso, como se vio en el apartado de antecedentes, para sustentar la reserva, el área manifestó expresamente que divulgar lo solicitado pondría en riesgo la seguridad informática de la institución por lo siguiente:

- Para garantizar la confiabilidad de un documento electrónico se hace uso de “Algoritmos o métodos de cifrado”, los cuales se encargan de transformar el contenido del documento en un

[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)

conjunto de caracteres sin orden o significado, con la finalidad de que la persona que tenga la llave o clave de acceso puede tener acceso al equipo y a la información contenida en el equipo.

- Para realizar el cifrado de un documento se pueden realizar diversos métodos de cifrado, lo que puede ser un procedimiento sencillo, o bien, el uso de algoritmos científicos y comerciales, para lo cual se realiza una gran cantidad de procesos de cómputo.
- Cuando se da a conocer el cifrado, se da a conocer el proceso de cifrado del documento, lo que permite, en su caso, acceder a la información de manera sencilla.
- Revelar el método de cifrado de cualquier documento, como puede ser comunicaciones, equipos de seguridad, cifrado de correo o cifrado de documentos, permitiría dar a conocer la técnica para proteger la información procesada en esos elementos de cómputo, lo que facilitaría un ataque para la obtención de información.

En dicho oficio, se agrega que de la información requerida en los incisos a), b), c), e) y f), se podrían presentar algunos riesgos, a saber:

- Informar los archivos almacenados en disco duro con algún cifrado y que son controlados por contraseña, así como indicar que los usuarios no pueden copiar ni borrar archivos sin necesidad de contar con privilegios o contraseñas, lo que pone en riesgo la integridad física de los usuarios en caso de algún robo premeditado o intencional para la extracción de información, a fin de tratar de obtener llaves de cifrado para extraer o manipular información contenida en los equipos, lo que, según refiere, encuadra en el artículo 113, fracción V de la Ley General de Transparencia.

- Dar a conocer los nombres comerciales de los sistemas informáticos utilizados para el cifrado de archivos puede permitir a los “ciber delincuentes” encontrar las llaves para su descifrado en el mercado negro.
- Los archivos almacenados en los equipos contienen información relacionada con las funciones desarrolladas por los servidores públicos el Alto Tribunal, en el ámbito de competencia que corresponda.
- En cuanto a la cantidad de puertos “USB”, la norma “ISO 27002”, que se refiere al estándar internacional para la seguridad de la información, indica diversas recomendaciones sobre prácticas en la gestión de la seguridad de la información para iniciar, implementar o mantener sistemas de gestión de la información, agrega que el uso de la información móvil implica considerar los riesgos de trabajar en entornos desprotegidos, estableciendo que se deben adoptar las medidas de seguridad adecuadas para la protección contra riesgos derivados del uso de los recursos informáticos, entre ellos, el uso de los dispositivos “USB”.
- Conforme al Acuerdo General de Administración IV/2008, la Dirección General de Tecnologías de la Información puede restringir el acceso a un recurso como los puertos “USB”, considerando las medidas de seguridad aplicables y reservándose la difusión de esas medidas, además, porque a través de esos puertos se puede insertar algún virus, programa informático o información maliciosa que perjudique a los servidores públicos y a la institución.

Ahora bien, como se adelantó, conforme a los argumentos reseñados se clasifica la información solicitada como **reservada**, al estimar actualizada la hipótesis del artículo 113, fracción I de la Ley General de Transparencia, bajo el argumento central de que se podría vulnerar la seguridad y operatividad de

la infraestructura tecnológica que sirve de apoyo al desarrollo de la operación de las áreas del Alto Tribunal, por lo que se transcribe ese precepto:

> ***"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;*
> (…)

Al respecto, se tiene en cuenta lo resuelto en la clasificación de información CT-CI/A-3-2018, en la que este Comité determinó que los datos de cada uno de los equipos de cómputo en posesión de la Suprema Corte de Justicia de la Nación atinentes a las características de tecnología, se debían clasificar como información reservada, de conformidad con el artículo 113, fracción I de la Ley General de Transparencia, entre ellos, lo relativo al número de serie.

Se afirma que se actualiza esa hipótesis, al considerar que la Dirección General de Tecnologías de la Información es el área técnica para pronunciarse sobre la información solicitada y ha señalado que se podría comprometer la seguridad informática al proporcionar la información solicitada en relación con el número de serie de cada uno de los equipos de cómputo, pues implicaría, por ejemplo, dar a conocer que los archivos almacenados en un disco duro que tienen algún cifrado y que son controlados por contraseña, así como indicar que los usuarios no pueden copiar ni borrar archivos sin necesidad de contar con privilegios o contraseñas, lo cual, se reitera, podría poner en riesgo la seguridad y operatividad de la infraestructura tecnológica que permite la operación de las diversas áreas del Alto Tribunal, ocurriendo lo mismo si se da a conocer los nombres comerciales de los sistemas informáticos utilizados para el cifrado de archivos, pues permitiría a los "ciber delincuentes" encontrar las llaves para su descifrado.

Para explicar esta conclusión, debe tenerse en cuenta que de conformidad con lo dispuesto en los artículos 100, último párrafo de la Ley General[2], en relación con el 17, párrafo primero Acuerdo General de Administración 5/2015[3], 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 reitera, 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 sistemas tecnológicos del Alto Tribunal, es claro que cuando el área enteramente responsable de ellos 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 igual manera, como se mencionó en la resolución CT-CI/A-3-2018, en este caso, este Comité de Transparencia identifica que se pretende proteger, desde un esquema global, los equipos de cómputo a través de los cuales se desarrollan las diversas actividades de la Suprema Corte de Justicia de la Nación, pues en el caso concreto, implicaría dar conocer si los archivos almacenados en disco duro con algún cifrado son controlados por contraseña, permitiendo acceder a la información contenida en esos equipos de cómputo,

---

[2] ***"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."

[3] ***"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…"

lo que potencializaría el nivel de vulnerabilidad de un ataque cibernético y suplantación de identidad.

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 es así, porque se podrían poner en riesgo cuestiones de seguridad pública, ya que, según se refirió previamente, dar a conocer si los archivos almacenados en un disco duro con algún cifrado son controlados por contraseña, en relación con el número de serie específico de cada equipo, así como indicar si los usuarios pueden copiar o borrar archivos sin necesidad de contar con privilegios o contraseñas, posibilitaría obtener diversa información que identificaría claramente las tecnologías, esquemas de conectividad y de seguridad, así como equipos y tecnologías que se emplean en el Alto Tribunal, facilitando acciones de posibles ataques cibernéticos.

En ese orden de ideas, se debe 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[4], de la Ley General de Transparencia.

---

[4] ***"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.

Lo anterior no implica una limitación al derecho de acceso a la información, en tanto que el conocimiento relacionado con las tecnologías y equipos de cómputo de este Alto Tribunal, así como cualquier otro tipo de bienes o servicios 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 poner en riesgo la seguridad informática del Alto Tribunal, ni la información contenida en dichos equipos o sistemas como ocurre en este caso[5].

Por lo expuesto y fundado; se,

R E S U E L V E:

ÚNICO. En la materia de análisis, se clasifica como reservada la información solicitada, de conformidad con lo señalado en la presente determinación.

Notifíquese al solicitante, a la instancia requerida y a la Unidad General de Transparencia.

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."

[5] *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".

Por unanimidad de votos lo resolvió el Comité de Transparencia de la Suprema Corte de Justicia de la Nación, integrado por el licenciado Alejandro Manuel González García, Secretario Jurídico de la Presidencia y Presidente 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.

LICENCIADO ALEJANDRO MANUEL GONZÁLEZ GARCÍA
PRESIDENTE DEL COMITÉ

MAGISTRADO CONSTANCIO CARRASCO DAZA
INTEGRANTE DEL COMITÉ

LICENCIADO JUAN CLAUDIO DELGADO ORTIZ MENA
INTEGRANTE DEL COMITÉ

LICENCIADO LUIS RAMÓN FUENTES MUÑOZ
SECRETARIO DEL COMITÉ