CUMPLIMIENTO CT-CUM-R/A-2-2019
Derivado del CT-CI/A-27-2018

Ciudad de México. Resolución del Comité de Transparencia de la Suprema Corte de Justicia de la Nación, correspondiente al trece de marzo de dos mil diecinueve.

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, respecto de lo cual, una vez desahogada la prevención, se requirió:

> *"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,"*

II. Respuesta del área. En respuesta a lo requerido, mediante oficio DGTI/DAPTI-2223-2018, la Dirección General de Tecnologías de la Información clasificó como reservados los datos requeridos en los incisos a), b), c), e) y f), señalando que esa información está relacionada con las medidas de seguridad internas, ya que detalla el 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 cada uno de los equipos del Alto Tribunal, de ahí que proporcionar esa información implicaría hacer público el esquema de seguridad que se tiene para tales equipos y pondría en riesgo tanto al personal, como a la Suprema Corte de Justicia de la Nación.

Por cuanto a la información requerida en el inciso d) de la solicitud de acceso, se informó que los equipos que se proporcionan a los servidores públicos del Alto Tribunal llevan enlistados los navegadores *"Microsoft Edge y Microsoft Internet Explorer"* y que le navegador *"Tor Browser"* no se encuentra instalado.

III. Resolución del Comité de Transparencia. En sesión de treinta y uno de octubre de dos mil dieciocho, este Comité de Transparencia emitió la resolución CT-CI/A-27-2018, en la que tuvo por atendida la solicitud respecto de lo solicitado en el inciso d) y confirmó la clasificación de reserva de la información requerida en los incisos a), b), c), e) y f), destacando que la difusión de esa información podría poner en riesgo cuestiones de seguridad pública, porque al darla a conocer posibilitaría obtener diversa información que identificaría claramente las tecnologías, esquemas de conectividad y de seguridad, así como equipos que se emplean en el Alto Tribunal, facilitando acciones de posibles ataques cibernéticos.

IV. Interposición del recurso de revisión. A través de la Plataforma Nacional de Transparencia, el veintitrés de noviembre de dos mil dieciocho, se interpuso recurso de revisión en contra de la resolución dictada por este Comité en el expediente CT-CI/A-27-2018 (fojas 37 a 40).

V. Notificación del recurso de revisión. El veintiséis de noviembre de dos mil dieciocho, mediante oficio INAI/STP/DGAP/1442/2018, la Directora General de Atención al Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales remitió a la Unidad General de Transparencia de este Alto Tribunal el recurso de revisión interpuesto por el peticionario (foja 36).

VI. Resolución del Instituto Nacional de Transparencia. El veinte de febrero de dos mil diecinueve, el Pleno del Instituto Nacional de Transparencia resolvió el recurso de revisión RRA 10276/18, determinando lo que se transcribe en la parte que interesa (fojas 97 a 105):

> *"Expuestas las posturas de las partes, este órgano de control democrático procede al análisis de la legalidad de la respuesta emitida a la solicitud motivo del presente recurso de revisión, a fin de determinar si el sujeto obligado garantizó el derecho de acceso a la información pública del particular, en razón del agravio expresado.*
>
> ***Clasificación en términos del artículo 110, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública.***
>
> *Al respecto, la Ley Federal de Transparencia y Acceso a la Información Pública establece lo siguiente:*
>
> (…)
>
> *De los preceptos normativos referidos, es posible desprender:*
>
> - *Podrá clasificarse como reservada aquella información cuya divulgación comprometa la seguridad nacional, la seguridad pública o la defensa nacional y cuente con un propósito genuino o un efecto demostrable.*
>
> - *Podrá clasificarse como información reservada, aquella que por disposición expresa de una ley tenga ese carácter, siempre que sea acorde con las bases, principios y disposiciones establecidas en la Ley General y Federal de Transparencia, así como las previstas en tratados internacionales, sin contravenirlas.*
>
> *A su vez, el Décimo Séptimo, fracción IV, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas –en adelante Lineamientos Generales-, dispone lo siguiente:*

(…)

Como se observa, de acuerdo a los Lineamientos en cita, se considera un riesgo a la seguridad nacional, la divulgación de aquella información a través de la cual se pueda obstaculizar o bloquear las actividades de inteligencia o contrainteligencia y cuando se revelan, entre otros, especificaciones técnicas, tecnología o equipos que sean útiles para la generación de inteligencia para la seguridad nacional.

Ahora bien, en ese sentido, el sujeto obligado en el caso que nos ocupa, manifestó que la información actualiza la fracción (sic) *113, fracción I de la Ley General de Transparencia y Acceso a la Información Pública, bajo el argumento central de que se podría vulnerar la seguridad y operatividad de la infraestructura tecnología* (sic) *que sirve de apoyo al desarrollo de la operación de las áreas del Alto Tribunal.*

Asimismo, la Dirección General de Tecnologías de la Información de la Suprema Corte de Justicia de la Nación, señaló 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 la operatividad de la infraestructura tecnológica, ocurriendo lo mismo, si se dan a conocer los nombres comerciales de los sistemas informáticos utilizados para el cifrado de los archivos, pus permitiría a los 'ciberdelincuentes' encontrar las llaves para su cifrado.

Ahora bien, de lo hasta ahora manifestado por el sujeto obligado, se puede apreciar que los argumentos tendentes a motivar la actualización de la fracción I del artículo 110 de la Ley Federal de Transparencia y Acceso a la Información Pública, no son aplicables, pues de los mismos no se desprende que la divulgación de la información de referencia efectivamente comprometa la seguridad nacional, la seguridad pública o la defensa nacional y cuente con un propósito genuino y demostrable, elementos que son necesarios invariablemente para actualizar la causal de reserva en estudio.

De igual forma, la publicación de la información no obstaculizaría las actividades de inteligencia o contrainteligencia, pues el sujeto obligado no tiene esas funciones destinadas.

En consecuencia, se determina que en el presente caso ***no se actualiza*** *la causal de reserva prevista en el artículo* ***110, fracción I*** *de la Ley Federal de Transparencia y Acceso a la Información Pública.*

No obstante, tomando en cuenta la naturaleza de la información y de los argumentos esgrimidos por el sujeto obligado en vía de alegatos, con fundamento en el artículo 147 de la Ley General de Transparencia y Acceso a la Información Pública, se procede a analizar la causal de reserva establecida en la ***fracción VII, del artículo 110,*** *de la Ley Federal de Transparencia y Acceso a la Información Pública, misma que prevé:*

> ***'Artículo 110.*** *Conforme a lo dispuesto por el artículo 113 de la Ley General, como información* ***reservada*** *podrá clasificarse aquella cuya publicación:*
> *…*
> ***VII.*** *Obstruya la prevención o persecución de los delitos;'*

En relación con tales disposiciones, los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, en lo sucesivo Lineamientos Generales, prevén lo siguiente:

> ***'Vigésimo sexto.*** *De conformidad con el artículo 113, fracción VII de la Ley General, podrá considerarse como información reservada, aquella que obstruya la prevención de delitos al obstaculizar 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.*
>
> *Para que se verifique el supuesto de reserva, cuando se cause un perjuicio a las actividades de persecución de los delitos, deben de actualizarse los siguientes elementos:*
>
> ***I.*** *La existencia de un proceso penal en sustanciación o una carpeta de investigación en trámite;*
>
> ***II.*** *Que se acredite el vínculo que existe entre la información solicitada y la carpeta de investigación, o el proceso penal, según sea el caso, y*
>
> ***III.*** *Que la difusión de la información pueda impedir u obstruir las funciones que ejerce el Ministerio Público o su equivalente durante la etapa de investigación o ante los tribunales judiciales con motivo del ejercicio de la acción penal.'*

De los preceptos normativos referidos, es posible desprender que como información ***reservada*** *podrá clasificarse aquella cuya publicación obstruya la prevención o persecución de los delitos.*

En esta tesitura, 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.***

Ahora bien, el artículo 104 de la Ley General de Transparencia y Acceso a la Información Pública, dispone que el invocar alguna de las causales de reserva previstas en el artículo 110 de la Ley Federal de la materia, el sujeto obligado deberá fundar y motivar tal cuestión, a través de la aplicación de la ***prueba de daño****, en la cual deberá justificar lo siguiente:*

- *La divulgación de la información representa un* ***riesgo real, demostrable e identificable*** *de perjuicio significativo al interés público o a la seguridad nacional;*

- *El riesgo de perjuicio que supondría la divulgación* ***supera el interés público*** *general de que se difunda, y*

- ***La limitación se adecua al principio de proporcionalidad*** *y representa el* ***medio menos restrictivo*** *disponible para evitar el perjuicio.*

En seguimiento a lo anterior, el numeral Trigésimo Tercero de los Lineamientos Generales señala que para la aplicación de la prueba de daño a la que hace referencia el artículo 104 de la Ley General de la materia, los sujetos obligados deberán atender lo siguiente:

- *Se deberá citar la fracción y, en su caso, la causal aplicable del artículo 113 de la Ley General, vinculándola con el Lineamiento específico y, cuando corresponda, el supuesto normativo que expresamente le otorga el carácter de información reservada.*

- *Mediante la ponderación de los intereses en conflicto, **los sujetos obligados deberán 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.*

- *Se debe acreditar el vínculo entre la difusión de la información y la afectación del interés jurídico tutelado de que se trate.*

- *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;*

- *En la motivación de la clasificación, el sujeto **obligado deberá acreditar las circunstancias de modo, tiempo y lugar del daño**, y*

- *Deberá 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.*

En tales términos, en el caso concreto, el sujeto obligado señaló en su alegatos diversas precisiones respecto de la información que originalmente clasificó en términos del artículo 110 de la Ley Federal de Transparencia y Acceso a la Información Pública, pero que resultan aplicables a la fracción VII del artículo citado, pues se le colocaría en estado de vulnerabilidad que permitiría el acceso ilícito a sus sistemas y equipos informáticos, facilitando una posible intervención de sus comunicaciones, la usurpación de sus permiso de red y la suplantación de sus equipos, afectando el ejercicio de sus labores cotidianas.

En las relatadas condiciones, este Instituto garante procederá a verificar si en el presente asunto se configuran los elementos aludidos en función de la reserva de la información que nos ocupa.

*Como punto de partida, es menester precisar que **de la causal de reserva en análisis se advierten dos vertientes**; el primero se refiere a la prevención de los delitos y el segundo a la persecución de los mismos.*

*En ese sentido, cabe puntualizar que, de conformidad con lo previsto en los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, la **obstrucción a la prevención de los delitos** deben vincularse con 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.*

*A mayor abundamiento, 'por definición de la palabra **prevención** 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 (…). Por consiguiente, 'prevención del delito' no es más que 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'*

*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'.*

Bajo tales consideraciones, cabe recordar que –en síntesis- las manifestaciones vertidas por el sujeto obligado, tienden a señalar que la difusión de la información requerida podría:

- ✓ *Comprometer la seguridad informática de la Suprema Corte de Justicia de la Nación.*
- ✓ *Potencializar el nivel de vulnerabilidad de un ataque cibernético.*
- ✓ *Suplantación de la identidad.*
- ✓ *Afectar los esquemas de conectividad y seguridad.*
- ✓ *Afectar el ejercicio de sus labores cotidianas.*

*Es decir, de los argumentos esgrimidos por la Suprema Corte de Justicia de la Nación se advierte que la negativa de acceso a la información se motivaría, en su caso, en pretender **prevenir la comisión de un delito de carácter cibernético que afectaría sus equipos y sistemas de informática**.*

Al respecto, el Código Penal Federal dispone lo siguiente sobre el acceso ilícito a sistemas y equipos de informática:

(…)

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

*Bajo esa óptica, en este punto, es necesario traer a colación, como **hechos notorios**, lo actuado durante la sustanciación de los diversos recursos de revisión con número de expediente **RRA 3628/18**, interpuesto en contra del Consejo de la Judicatura Federal y **RRA 7511/18** en contra del Centro de Investigación y Seguridad Nacional.*

(…)

*Al respecto, cabe señalar que el recurso de revisión **RRA 3628/18** derivó de la inconformidad que un particular hizo valer en contra de la respuesta que el Consejo de la Judicatura Federal brindó a la solicitud con número de folio 0320000111218, en la que se requirió información similar a la peticionada en la solicitud que nos ocupa en el caso concreto.*

Así, durante la tramitación de dicho expediente, se formuló una consulta a la Dirección General de Tecnologías de la Información de este Instituto, a efecto de que informara si de manera conjunta o aislada, la información solicitada pudiera vulnerar la seguridad de los equipos de manera remota, o si podría darse una

afectación a los servicios informáticos del sujeto obligado, al proporcionar los datos a los que se solicita acceso.

En atención a dicha consulta, el Titular de la Dirección General de Tecnologías de la Información de este Instituto, a través del oficio número INAI/SE/DGTI/344/2018, precisó que toda vez que se proporcionan datos informáticos sensibles como lo es el ***número de serie*** *de cualquier equipo informático en materia de tecnologías de la Información y Comunicación (TIC), de forma aislada éstos pueden representar un nivel de riesgo de seguridad mínimo para el sujeto obligado, el cual puede asumir al momento de dar a conocer los datos informáticos en comento.*

Sin embargo, añadió que ***cuando se proporciona un conjunto de datos informáticos de TIC sensibles y que además se encuentran correlacionados, como los peticionados****, con tal información cualquier persona con* ***fines malintencionados****, podría utilizar sus conocimientos para 'hackear' (acción de entrar de forma abrupta y sin permiso a un sistema de cómputo o una red) o crackear (literalmente traducido como rompedor, del inglés ' to track', que significa romper o quebrar) se utiliza para referirse a las personas que rompen o vulneran algún sistema de seguridad, los sistemas informáticos objetivo y de alguna manera correlacionan la información para* ***vulnerar la seguridad de los equipos informáticos así como afectar los servicios informáticos del sujeto obligado.***

Por otro lado, durante la sustanciación del recurso de revisión ***RRA 7511/18****, de la misma manera, se formuló una consulta a la Dirección General de Tecnologías de la Información. En desahogo a dicha consulta, esa Unidad Administrativa precisó lo siguiente:*

- ✓ *Que en criptografía, el cifrado es un procedimiento que utiliza un algoritmo con 'clave descifrado' para transformar un mensaje, sin atender a su estructura lingüística o significado, de tal forma que sea incomprensible o, al menos, difícil de comprender a toda persona que no tenga la clave de cifrado del algoritmo. Las claves de cifrado y descifrado pueden ser simétricas, asimétricas o híbridas.*
- ✓ *Que dentro de las Tecnologías de la Información y Comunicación, el* ***cifrado de disco duro proporciona una capa de seguridad con la finalidad de proteger información sensible*** *y que únicamente aquellas personas que posean la clave de cifrado puedan leer y editar información. Por tanto, el cifrado de disco duro protege la información contenida dentro del mismo, en el caso de que una persona ajena tenga acceso físico a nuestro equipo.*
- ✓ *Por otro lado, si se extrae el disco duro y éste es montado en otro equipo de cómputo, la información contenida dentro de su interior no podrá ser leída.*

Asimismo, específicamente, respecto del cuestionamiento consistente en ¿Dar a conocer si los archivos almacenados están cifrados, y los nombres comerciales de los programas informáticos para el cifrado utilizados por el sujeto obligado, representan un riesgo a los sistemas, redes o equipos del sujeto obligado?, la Dirección General de Tecnologías la Información de este Instituto señaló que:

(…)

Tomando en consideración lo anterior, se concluye que con la publicidad de (sic) *del 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 su posesión, ***se podría generar un riesgo potencial para la infraestructura tecnológica de la Suprema Corte de Justicia de la Nación****, ya que pueden ser utilizadas para propiciar* ***ataques informáticos de diversa índole.***

Así, este Instituto considera que la entrega de dichos datos, se ocasionaría lo siguiente:

I. *Un potencial* ***riesgo real, demostrable e identificable*** *a la Suprema Corte de Justicia de la Nación, toda vez que se le colocaría en un estado* ***de vulnerabilidad*** *que permitiría el acceso a sus sistemas y equipos informáticos, facilitando:*

- ***a.*** *Una posible intervención de sus comunicaciones,*
- ***b.*** *La usurpación de sus permisos,*
- ***c.*** *La suplantación de sus equipos y de la información que almacena en sus servidores;*
- ***d.*** *El robo de la información que obra en sus archivos digitales, y*
- ***e.*** *El detrimento de sus instalaciones tecnológicas.*

Cuestiones que se materializan con la comisión de delitos de carácter cibernético, que sin duda afectarían severamente el ejercicio de las labores cotidianas y sustantivas de la Suprema Corte de Justicia de la Nación.

II. *Un* ***perjuicio significativo al interés público****, ya que se pondría en riesgo su responsabilidad fundamental en la defensa del orden establecido por la Constitución Política de los Estados Unidos Mexicanos, a través de los medios de control constitucional.*

Con base en lo anterior, ***el riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda la información****, ya que el resguardo de los datos consistentes en los* ***números de serie*** *de los equipos de cómputo y los* ***nombres comerciales de los programas informáticos utilizados para el cifrado de los archivos*** *instalados en los equipos de la dependencia, implica llevar a cabo la* ***prevención del delito de acceso ilícito a sistemas y equipos de informática tipificado en el Código Penal Federal****, lo cual cobra importancia si se considera que dicha conducta implica conocer, copias, modificar, destruir o provocar la pérdida de información contenida en sistemas o equipos de informática.*

En consecuencia, al revelar dichos datos no sólo se comprometería la información que obra en los archivos digitales del sujeto obligado, sino que menoscabaría la seguridad y certeza de los ciudadanos que acuden a éste para otorgar certeza respecto de la impartición de justicia y control constitucional.

Asimismo, la ***limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio,*** *toda vez que* ***la pretensión de fondo que persigue la reserva de la información consiste en prevenir la conducta antijurídica tipificada*** *(acceso ilícito a sistemas y equipos de informática), misma que de llevarse a cabo podría permitir la realización de diversos* ***ataques*** *a la infraestructura tecnológica y de sistemas del sujeto obligado.*

*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 la 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.*

Ahora bien, en relación al periodo de reserva, el segundo párrafo del artículo 99 de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el Trigésimo Cuarto de los Lineamientos Generales, disponen que la información clasificada podrá permanecer con tal carácter hasta por un periodo de cinco años.

(…)

Así, en el caso concreto, este Instituto considera pertinente, tal y como lo solicitó el Comité de Transparencia del sujeto obligado, reservar la información requerida por el particular por un periodo de cinco años, pues a juicio de este Organismo Garante dicho plazo es proporcional a la naturaleza y el grado de especificidad del tipo de información de que se trata.

(…)

*En tales condiciones, tomando en consideración que no se acreditó la clasificación de la información en los términos aludidos por el Comité de Transparencia del sujeto obligado, es posible concluir que el agravio formulado por el particular resulta **parcialmente fundado.***

***CUARTA. Decisión.** Con fundamento en el artículo 157, fracción III de la Ley Federal de Transparencia y Acceso a la Información Pública, este Instituto considera procedente **modificar** la respuesta de la Suprema Corte de Justicia de la Nación e **instruirle** para que en un plazo máximo de diez días hábiles, a través de su Comité de Transparencia, confirme 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 se*

pueden borrar o no archivos con o sin contraseña 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 la ***fracción VII, del artículo 110*** *de la Ley Federal de Transparencia y Acceso a la Información Pública, por un periodo de 5 años, debiendo cumplir con la debida fundamentación, motivación y prueba de daño."*

(…)

VII. Remisión del expediente a la Secretaría del Comité de Transparencia. Mediante oficio UGTSIJ/TAIPDP/0776/2019, el seis de marzo de dos mil diecinueve, el Titular de la Unidad General de Transparencia y Sistematización de la Información Judicial remitió a la Secretaría del Comité de Transparencia el testigo del expediente UT-A/0382/2018, a fin de que este Comité se pronuncie sobre el cumplimiento de la resolución dictada por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

VIII. Acuerdo de turno. Mediante proveído de seis de marzo de dos mil diecinueve, la Presidencia del Comité de Transparencia de este Alto Tribunal, con fundamento en los artículos 44, fracción I de la Ley General de Transparencia y Acceso a la Información Pública y 23, fracción I y 27 del Acuerdo General de Administración 5/2015, ordenó integrar el expediente **CT-CUM-R/A-2-2019** y, conforme al turno correspondiente, remitirlo al Contralor del Alto Tribunal, por ser ponente de la resolución precedente, a fin de que presentara la propuesta sobre el cumplimiento de la resolución dictada por el Instituto Nacional de Transparencia, lo que se hizo mediante oficio CT-526-2019 el siete de marzo de este año.

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

I. Competencia. El Comité de Transparencia de la Suprema Corte de Justicia de la Nación es competente para confirmar, modificar o revocar las determinaciones de clasificación de información, de conformidad con los

artículos 6° de la Constitución Política de los Estados Unidos Mexicanos; 44, fracción II, de la Ley General; 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública (Ley Federal), y 23, fracción II, del Acuerdo General de Administración 5/2015.

Además, la competencia a cargo de este Comité surge de la propia resolución del recurso de revisión **RRA 10276/18**, de veinte de febrero de dos mil diecinueve, emitida por el Instituto Nacional de Transparencia, en términos de los artículos 151, párrafo segundo y 157 de la Ley General de Transparencia.

II. Análisis. Como se advierte del antecedente I, en la solicitud que da origen a este asunto se pidió 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 informara 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.

En seguimiento de esa solicitud, en el expediente CT-CI/A-27-2018, se confirmó la clasificación de reserva de los datos requeridos en los incisos a),

b), c), e) y f), por estimarse actualizada la hipótesis prevista en el artículo 113, fracción I de la Ley General de Transparencia y Acceso a la Información Pública; además, se tuvo por atendida la solicitud respecto de lo pedido en el inciso d).

Ahora bien, en la resolución dictada por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales en el recurso de revisión RRA 10276/18, se determinó, en esencia, lo siguiente:

- No se actualiza la causal de reserva prevista en el artículo 110, fracción I de la Ley Federal de Transparencia, esto es, por seguridad nacional, respecto del número de serie de los equipos, conocer si los discos duros se encuentran encriptados, nombre comercial de los programas de encriptado de información, conocer si se pueden borrar o no archivos con o sin contraseña, y conocer si se puede almacenar información a través de los puertos USB, de cada uno de los equipos de cómputo en posesión del Alto Tribunal.

- Se actualiza la causal de reserva prevista en el artículo 110, fracción VII de la Ley Federal de la materia, consistente en la obstrucción a la prevención de delitos, respecto de los datos referidos el punto anterior.

En cumplimiento de lo determinado por el Instituto Nacional de Transparencia, en el sentido de que este Comité debe dictar una resolución en la que confirme la reserva temporal de la información solicitada con fundamento en la fracción VII del artículo 110 de la Ley Federal de Transparencia y Acceso a la Información Pública, se procede a emitir el pronunciamiento correspondiente, por lo que se transcribe dicho artículo:

> *"**Artículo 110.** Conforme a lo dispuesto por el artículo 113 de la Ley General, como información reservada podrá clasificarse aquella cuya publicación:*
> (…)
> ***VII.** Obstruya la prevención o persecución de los delitos;"*
> (…)

Sobre el alcance de dicho precepto, en la resolución emitida en el recurso de revisión que se cumplimenta, se señala que *"como información reservada podrá clasificarse aquella cuya publicación obstruya la prevención o persecución de delitos",* agregando que *"para que pueda acreditarse que la información requerida pudiera 'obstruir la prevención de los delitos', debe vincularse a la* ***afectación a las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de las autoridades para evitar la comisión de delitos"*** (página 98, vuelta).

Además, se precisa que de esa causal de reserva se desprenden dos vertientes: una que se refiere a la prevención de los delitos y la otra a la persecución de los mismos, agregando: *"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".*

Enseguida se hace alusión al Código Penal Federal señalando que *"comete el* ***delito de acceso ilícito a sistemas y equipos de informática*** *todo aquel que* ***sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática***

***protegidos por algún mecanismo de seguridad**, sean o no propiedad del Estado. Asimismo, al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del **Estado**, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa"* (foja 100 vuelta).

Adicionalmente, es de destacar que en la resolución emitida por el Instituto Nacional de Transparencia que se atiende, se invoca como hecho notorio, las respuestas que la Dirección General de Tecnologías de la Información de ese Instituto emitió en respuesta a las consultas que se le formularon sobre información similar a la de la materia de la solicitud que da origen a este asunto.[1]

En virtud de lo anterior, en la resolución se argumenta que *"derivado de la naturaleza y el grado de especificidad del tipo de información que se requiere, y que se trata de un elemento relevante al ponderar cualquier*

---

[1] *"Sin embargo, añadió que **cuando se proporciona un conjunto de datos informáticos de TIC sensibles y que además se encuentran correlacionados, como los peticionados**, con tal información cualquier persona con **fines malintencionados**, podría utilizar sus conocimientos para 'hackear' (acción de entrar de forma abrupta y sin permiso a un sistema de cómputo o una red) o crackear (literalmente traducido como rompedor, del inglés ' to track', que significa romper o quebrar) se utiliza para referirse a las personas que rompen o vulneran algún sistema de seguridad, los sistemas informáticos objetivo y de alguna manera correlacionan la información para **vulnerar la seguridad de los equipos informáticos así como afectar los servicios informáticos del sujeto obligado"*** (foja 101 vuelta).

En el desahogo de diversa consulta, la citada unidad administrativa expuso:

- ✓ *"Que en criptografía, el cifrado es un procedimiento que utiliza un algoritmo con 'clave descifrado' para transformar un mensaje, sin atender a su estructura lingüística o significado, de tal forma que sea incomprensible o, al menos, difícil de comprender a toda persona que no tenga la clave de cifrado del algoritmo. Las claves de cifrado y descifrado pueden ser simétricas, asimétricas o híbridas.*
- ✓ *Que dentro de las Tecnologías de la Información y Comunicación, el **cifrado de disco duro proporciona una capa de seguridad con la finalidad de proteger información sensible** y que únicamente aquellas personas que posean la clave de cifrado puedan leer y editar información. Por tanto, el cifrado de disco duro protege la información contenida dentro del mismo, en el caso de que una persona ajena tenga acceso físico a nuestro equipo.*
- ✓ *Por otro lado, si se extrae el disco duro y este es montado en otro equipo de cómputo, la información contenida dentro de su interior no podrá ser leída."*

De igual forma, respecto del cuestionamiento "*¿Dar a conocer si los archivos almacenados están cifrados, y los nombres comerciales de los programas informáticos para el cifrado utilizados por el sujeto obligado, representan un riesgo a los sistemas, redes o equipos del sujeto obligado?"*, la dirección general en comento refirió (foja 102):

> *"Cuando se proporciona un conjunto de datos informáticos de TIC sensibles y que además se encuentran correlacionados como por ejemplo: **nombres comerciales de los programas informáticos para cifrar**, método de cifrado, tipo de cifrado, longitud de las llaves, etc., con tal información **cualquier persona con fines malintencionados, podría utilizar sus cocimientos o contratar alguna persona con capacidades y conocimientos en materia de hackear"***
> (…)

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",* conforme al artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en específico, la obstrucción a la prevención de delitos.

De conformidad con lo expuesto, atendiendo a los argumentos señalados por el Instituto Nacional de Transparencia, este Comité de Transparencia **confirma la clasificación de reserva** de la información relativa al número de serie; conocer si los discos duros se encuentran encriptados; 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 de la Suprema Corte de Justicia de la Nación, con fundamento en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, dado que como se hizo valer en la resolución dictada en el expediente CT-CI/A-27-2018, considerando que la Dirección General de Tecnologías de la Información es el área técnica para pronunciarse sobre la información solicitada y señaló 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, 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 privilegios o contraseñas, podría poner en riesgo la seguridad operativa 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 los archivos.

Dado que, conforme a la argumentación sostenida en la resolución del Instituto Nacional de Transparencia que se atiende la reserva de dicha información permite prevenir la comisión del delito de acceso ilícito a sistemas y equipos de informática tipificados en el Código Penal Federal, pues al dar a conocer la información solicitada, no sólo se *"comprometería la información que obra en los archivos digitales del sujeto obligado, sino que menoscabaría la seguridad y certeza de los ciudadanos que acuden a éste para otorgar certeza respecto de la impartición de justicia y control constitucional".*

Por lo tanto se confirma se confirma la reserva de la información requerida, en los incisos a), b), c), e) y f) de la solicitud, con fundamento en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Análisis específico de la prueba de daño. En el caso, de acuerdo con el alcance de la causa de reserva prevista en el artículo 110, fracción VI de la Ley Federal de Transparencia y en términos de lo señalado por el Instituto Nacional de Transparencia en el recurso de revisión que se atiende, se determina (fojas 102 vuelta y 103):

La divulgación de la información solicitada conllevaría un riesgo real, demostrable e identificable, en tanto que colocaría a la Suprema Corte de Justicia de la Nación en un estado de vulnerabilidad, facilitando una posible intervención de las comunicaciones; usurpación de permisos; suplantación de equipos y de la información almacenada en los servidores; robo de

información que obran en los archivos digitales, así como el detrimento de las instalaciones tecnológicas.

En ese sentido, el perjuicio significativo al **interés público** resulta **menos restrictivo**, porque se pondría en riesgo la responsabilidad fundamental del Alto Tribunal en la defensa del orden establecido en la Constitución Federal, mediante los medios de control constitucional.

Por lo anterior, acorde con la resolución que se atiende se determinó que *"**el riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda la información**, ya que el resguardo de los datos consistentes en los **números de serie** de los equipos de cómputo y los **nombres comerciales de los programas informáticos utilizados para el cifrado de los archivos** instalados en los equipos de la dependencia, implica llevar a cabo la **prevención del delito de acceso ilícito a sistemas y equipos de informática tipificado en el Código Penal Federal**, lo cual cobra importancia si se considera que dicha conducta implica conocer, copias, modificar, destruir o provocar la pérdida de información contenida en sistemas o equipos de informática"*, por lo que revelar dichos datos *"no sólo se comprometería la información que obra en los archivos digitales del sujeto obligado, sino que menoscabaría la seguridad y certeza de los ciudadanos que acuden a éste para otorgar certeza respecto de la impartición de justicia y control constitucional".*

Ahora bien, dicha clasificación de reserva *"**se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio,** toda vez que **la pretensión de fondo que persigue la reserva de la información consiste en prevenir la conducta antijurídica tipificada** (acceso ilícito a sistemas y equipos de informática)",* de llevarse a cabo podría permitir la ejecución de diversos **ataques** a la infraestructura tecnológica y de sistemas con que cuenta este Alto Tribunal, ya que la difusión de los documentos solicitados *"**incrementa sustancialmente la posibilidad de que aquella persona que conozca***

dicha información cometa algún ilícito”, pues tendría acceso a información con un alto grado de precisión técnica, así como a los protocolos de seguridad y las características de la infraestructura instalada (foja 103).

Plazo de reserva. Finalmente, en términos de lo señalado en el artículo 101[2], párrafo segundo de la Ley General de Transparencia, se determina que el plazo de reserva será por cinco años, ya que por las consideraciones expuestas en la resolución del Instituto Nacional de Transparencia, mismas que se retoman en esta determinación, *“dicho plazo es proporcional a la naturaleza y el grado de especificidad del tipo de información de que se trata”.*

En cumplimiento de la determinación del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales hágase del conocimiento del solicitante esta determinación, la cual también deberá hacerse llegar a ese órgano garante, ya que contiene los motivos que sustentan la clasificación de reserva en los términos expuestos en el recurso de revisión que se atiende respecto de la información requerida.

Por lo expuesto y fundado; se,

R E S U E L V E:

PRIMERO. Se confirma la clasificación de reserva temporal de la información materia del recurso de revisión que se cumplimenta, acorde con lo señalado en esta resolución.

---

[2] ***“Artículo 101.*** *Los Documentos clasificados como reservados serán públicos cuando:*
…
La información clasificada como reservada, según el artículo 113 de esta Ley, podrá permanecer con tal carácter hasta por un periodo de cinco años. El periodo de reserva correrá a partir de la fecha en que se clasifica el documento…”

SEGUNDO. De conformidad con lo expuesto en la presente resolución, se atiende lo determinado por el Instituto Nacional de Transparencia.

TERCERO. Se instruye a la Unidad General de Transparencia informar lo conducente al Instituto Nacional de Transparencia y al solicitante, así como realizar las acciones necesarias para atender este asunto.

Notifíquese a la persona solicitante, al Instituto Nacional de Transparencia y a las instancias involucradas.

Por unanimidad de votos lo resolvió el Comité de Transparencia de la Suprema Corte de Justicia de la Nación, integrado por el licenciado Juan Sebastián Francisco de Asís Mijares Ortega, Director General de Asuntos Jurídicos y Presidente del Comité, y el licenciado Christian Heberto Cymet López Suárez, Contralor del Alto Tribunal. Ausente el titular de la Unidad General de Enlace con los Poderes Federales; quienes firman con el secretario del Comité que autoriza.

LICENCIADO JUAN SEBASTIÁN FRANCISCO DE ASÍS MIJARES ORTEGA
PRESIDENTE DEL COMITÉ

LICENCIADO CHRISTIAN HEBERTO CYMET LÓPEZ SUÁREZ
INTEGRANTE DEL COMITÉ

LICENCIADO ARIEL EFRÉN ORTEGA VÁZQUEZ
SECRETARIO DEL COMITÉ