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

CUMPLIMIENTO CT-CUM/A-20-2023
derivado del expediente **CT-CI/A-11-2018**

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 **veintiuno de junio de dos mil veintitrés.**

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

I. Solicitud de información. El diecisiete de mayo de dos mil dieciocho se recibió a través de la Plataforma Nacional de Transparencia la solicitud tramitada bajo el folio **0330000106518**, 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. Ordenado por Número de serie, de cada uno de los equipos de cómputo, y de cada uno de los MODEMS, ROUTERS (rúters) o Puntos de acceso inalámbricos, en posesión del sujeto obligado. a. Una relación de todos los puertos de red abiertos. b. Nombre y versión, del programa informático instalado para administrar o controlar lo referente al cortafuegos o firewall (en inglés). c. Si se encuentra habilitada la conexión de red IPv6 (Protocolo de Internet versión 6).*
> *Otros datos para facilitar su localización*
> *AMPARO INDIRECTO 408/2018 SEGUNDO de DISTRITO"* (sic)

II. Acuerdo de prevención. El dieciocho de mayo de dos mil dieciocho, el Subdirector General de la Unidad General de Transparencia y Sistematización de la Información Judicial, pidió al solicitante que precisara el tipo de documento e instancia del amparo indirecto aludido en su solicitud, y qué es lo que concretamente requiere de dicho expediente.

S4HrwykCIT99PZ1r51UQZihDV8v2kbcaKw0UylkHG3M=

III. Desahogo de la prevención. El veintinueve de mayo de dos mil dieciocho, el solicitante aclaró que la única información pública requerida es la siguiente:

> *"(…) 1. Ordenado por número de serie, de cada uno de los equipos de cómputo, y de cada uno de los MODEMS, ROUTERS (ruters) o Puntos de acceso inalámbricos, en posesión del sujeto obligado.*
> *a. El registro de todos los puertos de red abiertos.*
> *b. Nombre y versión del programa informático instalado para administrar o controlar lo referente al cortafuegos o firewall (en inglés).*
> *c. Si se encuentra habilitada la conexión de red IPv6 (Protocolo de internet versión 6).*
> *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. Solicitud de información. El treinta de enero de dos mil dieciocho se recibió a través de la Plataforma Nacional de Transparencia la solicitud tramitada bajo el folio **0330000114618**, 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. Ordenado por Número de serie, de cada uno de los equipos de cómputo y de cada uno de los MODEMS, ROUTERS (rúters) o Puntos de acceso inalámbricos, en posesión del sujeto obligado. a. Nombre de aquellas personas físicas que cuentan con las contraseñas administrativas o su equivalente (permisos informáticos, credenciales administrativas, privilegios de superusuario 'su', 'root', etc) para el manejo, administración y control de la configuración de cada equipo. b. Tipo de contratación, empleo, cargo o comisión que desempeñan las personas que resulten del inciso a. c. Forma en que cada equipo contiene 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 DHCOP, por sus siglas en inglés Dynamic Host Configuration Protocol). d. Domicilio actual en donde se encuentra físicamente cada equipo.*

V. Admisión de las solicitudes. En auto de treinta de mayo de dos mil dieciocho, la Unidad de Transparencia analizó la naturaleza y contenido de las solicitudes y las estimó procedentes, por lo que ordenó abrir los expedientes UT-A/0198/2018 (solicitud 0330000106518) y UT-A/0200/2018 (solicitud 0330000114618).

VI. Acumulación de las solicitudes. En acuerdo de once de junio de dos mil dieciocho el entonces Presidente del Comité de Transparencia de este Alto

S4HrwykClT99PZ1r51UQZihDV8v2kbcaKw0UylkHG3M=

Tribunal en términos de lo dispuesto en el artículo 3, párrafo segundo y 4 segundo párrafo, de los Lineamientos Temporales para Regular el Procedimiento Administrativo Interno de Acceso a la Información Pública, así como el Funcionamiento y Atribuciones del Comité de Transparencia de la Suprema Corte de Justicia de la Nación determinó acumular los expedientes UT-A-/200/2018 y UT-A-/0198/2018, toda vez que fue requerida información de la misma naturaleza, por la misma persona solicitante que también fueron respondidas por la Dirección General de Tecnologías de la Información, quien determinó la clasificación de la información, ello con el fin de privilegiar un procedimiento expedito, aunado a que advirtió con claridad que los hechos, es decir, la información y respuestas tienen el mismo efecto, pretendiendo evitar que se pudieren generar resoluciones contradictorias.

VII. Resolución del Comité de Transparencia de la Suprema Corte de Justicia de la Nación. En sesión de veintisiete de junio de dos mil dieciocho, este Comité de Transparencia emitió resolución en el expediente **CT-CI/A-11-2018**[1], en los siguientes términos:

> *"…**II. Análisis.** En principio se debe tener presente que el marco constitucional del derecho de acceso a la información comprende la posibilidad de cualquier persona de solicitar, investigar, difundir, buscar y recibir información que se encuentre integrada exclusivamente en documentos que refiere el ejercicio de sus atribuciones, en términos de las leyes Generales y Federal de la Materia.*
>
> *En el caso, el peticionario solicita obtener la información que se precisa a continuación -ordenada por número de serie, de cada uno de los equipos de cómputo, y de cada uno de los módems, routers o puntos de acceso inalámbricos-.*
>
> - *Una relación de todos los puertos de red abiertos.*
> - *Nombre y versión, del programa informático instalado para administrar o controlar lo referente al cortafuegos o firewall (en inglés).*
> - *Si se encuentra habilitada la conexión de red IPv6 (protocolo de Internet versión 6).*
> - *Nombre de aquellas personas físicas que cuentan con las contraseñas administrativas o su equivalente (permisos*

[1] Disponible en: CT-CI-A-11-2018.pdf (scjn.gob.mx)

S4HrwykCIT99PZ1r51UQZihDV8v2kbcaKw0UylkHG3M=

informáticos, credenciales administrativas, privilegios de superusuario 'su' 'root', etc.) para el manejo, administración y control de la configuración de cada equipo. Tipo de contratación, empleo, cargo o comisión que desempeñan las personas que resultan del inciso a.

- *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 DHCP, por sus siglas en inglés Dynamic Host Configuration Protocol).*
- *Domicilio actual en que se encuentra cada físicamente* (sic) *cada equipo"*

En respuesta, el Director General de Seguridad (sic) señaló que la información solicitada es de carácter reservado, con fundamento en el artículo 113, fracción I de la Ley General de Transparencia y Acceso a la Información Pública; ya que son datos que deben tratarse con mucha cautela y no pueden entregarse, debido a que ponen en riesgo la información contenida en los equipos de este Alto Tribunal; quedando altamente vulnerables y sin protección; fundándose en lo determinado por este Comité al resolver los expedientes CT-CI/A-3-2018 y CT-CI/A-5-2018, en las sesiones públicas ordinarias celebradas los días dieciocho de abril y dos de mayo, ambos de dos mil dieciocho.

Lo anterior, al puntualizar que proporcionar cualquier dato o elemento que lleve a obtener información de acceso a los anales de comunicación de este Alto Tribunal puede:

- *Generar en sí un alto riesgo de vulnerabilidad, como lo sería: a) dar a conocer si se cuenta con cierto tipo de tecnología; b) el equipo que se usa; c) su ubicación; d) número de serie; e) marca; f) contraseñas; g) sitios; h) esquemas de conectividad y de seguridad; i) puertos abiertos, j) nombre de los programas informáticos de los firewall y conexiones de red IP; y k) los nombres de las personas físicas y los procedimientos que realizan para la operación, ya que todos estos elementos sirven para salvaguardar la información y comunicaciones que hacen uso del sistema de comunicaciones, y entregar alguno de ellos podrían poner en riesgo cuestiones de seguridad pública y con ello, el acceso a la justicia.*
- *Traer las siguientes consecuencias: a) 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; b) exponer la capacidad de la red ante posibles ataques informáticos, porque se identificaría o remitiría información*

S4HrwykCIT99PZ1r51UQZihDV8v2kbcaKw0UylkHG3M=

> *contenida en los equipos, servidores, equipos de comunicación, atentando a la seguridad y conectividad tecnológica que se tiene implementada; c) con la información requerida en su conjunto permitir que cualquier persona capacitada ingrese a los sistemas de comunicación y a la información que se aloje en estos sistemas; d) cualquier afectación al Alto Tribunal pondría de igual forma en riesgo a las otras instancias del Poder Judicial de la Federación.*

En ese orden, el objeto de estudio de esta determinación se centra en analizar la clasificación de reserva realizada por el área vinculada sobre los datos requeridos, de conformidad con lo previsto por el artículo 113, fracción I, de la Ley General de transparencia y Acceso a la Información Pública, 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; […]'*

Al efecto, resulta necesario destacar que este órgano colegiado en la Clasificación de Información CT-CI/A-5-2018, validó la clasificación que la Dirección General de Tecnologías de la Información realizó a 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 del Alto Tribunal, reservándola en términos de la fracción I, del artículo 113, de la Ley General de Transparencia y Acceso a la Información Pública.

Lo anterior, en tanto que, desde la perspectiva del área técnica responsable, entregar dichos datos expone su capacidad de reacción ante posibles ataques cibernéticos y compromete un aspecto de la seguridad pública en general, ya que a parte del uso del número de serie o de parte de los módems, routers o puntos de acceso inalámbricos, sería posible dar o remitir diversa información que identifica las tecnologías, esquemas de conectividad y de seguridad, así como equipos y tecnologías que se emplean en el Alto Tribunal para salvaguardar la información de los sistemas de comunicaciones de la Suprema Corte de Justicia.

Atento a las consideraciones anteriores, y toda vez que en el caso que nos ocupa el área técnica, que cuenta con el personal especializado para velar por la seguridad de la información contenida en los sistemas tecnológicos del Alto Tribunal precisa que dar a conocer los datos requeridos pondría en riesgo cuestiones se seguridad pública y con ello, el acceso a la justicia

S4HrwykCIT99PZ1r51UQZihDV8v2kbcaKw0UylkHG3M=

> *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; este órgano colegiado procede a confirmar su reserva.*
>
> *Lo anterior se actualiza desde la especificidad que en aplicación de la prueba de daño disponen los artículos 103 y 104, de la Ley General de Transparencia, ya que, como se refirió, con la divulgación de la información que se analiza, se podrían identificar las tecnologías, esquemas de conectividad y de seguridad, que se emplean en la Suprema Corte para salvaguardar la información contenida en los sistemas de comunicaciones de este Alto Tribunal, poniendo en riesgo cuestiones de seguridad pública.*
>
> *En ese contexto, este órgano colegiado considera que, respecto a la información requerida, se actualiza la causal de reserva prevista en el artículo 113, fracción I de la Ley General de Transparencia y Acceso a la Información Pública, por un plazo de cinco años, atendiendo a lo establecido en el artículo 101, de la Ley General.*
>
> *Por lo expuesto y fundado; se.*
>
> ***RESUELVE:***
>
> ***ÚNICO.** Se confirma la clasificación de reserva efectuada por la Dirección General de Tecnologías de la Información, en los términos de esta determinación.*
>
> *…”*

VIII. Recurso de revisión. El treinta de julio de dos mil dieciocho, la persona solicitante interpuso ante el Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (INAI) los recursos de revisión en contra de las respuestas emitidas por la Unidad General de Transparencia en las solicitudes de información **0330000106518** y **0330000114618.**

En resolución de treinta y uno de octubre de dos mil dieciocho, en los Expedientes: RRA 6063/18 que acumula al RRA 6064/18, el INAI determinó lo siguiente:

> *“ (…)*
>
> *En ese orden de ideas, cabe precisar que, en el caso que nos ocupa, la información reservada por el sujeto obligado consiste en lo siguiente:*
>
> *1. Ordenado por Número de serie, de cada uno de los equipos de cómputo, y de cada uno de los MODEMS, ROUTERS (ruters) o Puntos de acceso inalámbricos, en posesión del sujeto obligado.*
>
> *2. Una relación de todos los puertos de red abiertos.*

S4HrwykClT99PZ1r51UQZihDV8v2kbcaKw0UylkHG3M=

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

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

5. Nombre de las personas físicas que cuentan con las contraseñas administrativas o su equivalente (permisos informáticos, credenciales administrativas, privilegios de superusuario "su", "root", etc.) para el manejo, administración y control de la configuración de cada equipo.

6. ***Tipo de contratación, empleo, cargo o comisión que desempeñan las personas que resulten del punto anterior.***

7. 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 (DHCP),

8. El domicilio actual en donde se encuentra físicamente cada equipo.

[…]

Así, la clasificación de la información obedece a que, a su parecer, se podría obstaculizar o bloqueen las actividades de inteligencia o contrainteligencia y cuando se revelen normas, procedimientos, métodos, fuentes, especificaciones técnicas, tecnología, equipo que sean útiles para la generación de inteligencia para la seguridad nacional.

[…]

En ese contexto, tomando en consideración las causales previstas en la prueba de daño que el sujeto obligado mencionó en la respuesta, a fin de sustentar la clasificación de la información, se tiene que éste refirió que al divulgar la información solicitada en la solicitud de acceso que nos ocupa, se estaría causando lo siguiente:

- *Que se pondrían en riesgos cuestiones de seguridad pública y con ello, el acceso a la justicia.*
- *Que se pondrían* [sic] *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.*

S4HrwykCIT99PZ1r51UQZihDV8v2kbcaKw0UylkHG3M=

- ✓ *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.*
- ✓ *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 estos sistemas.*
- ✓ *Se pondría 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.*

❖ *Que aunado a lo anterior, se podrían identificar las tecnologías, esquemas de conectividad y de seguridad, que se emplean en la Suprema Corte de Justicia de la Nación para salvaguardar la información contenida en los sistemas de comunicaciones de ese Alto Tribunal, poniendo en riesgo cuestiones de seguridad pública.*

❖ *Que 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.*

De lo anterior, se desprende que el sujeto obligado argumentó que si bien existe un riesgo al difundir lo requerido, ya que se podrían identificar las tecnologías, esquemas de conectividad y de seguridad, que se emplean en la Suprema Corte de Justicia de la Nación para salvaguardar la información contenida en los sistemas de comunicaciones de ese Alto Tribunal, poniendo en riesgo cuestiones de seguridad pública.

En resumen, este Instituto considera que en el presente caso, la divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público, ya que pudiera obstaculizar o bloqueen las actividades de inteligencia o contrainteligencia y cuando se revelen normas, procedimientos, métodos, fuentes, especificaciones técnicas, tecnología o equipo que sean útiles para la generación de inteligencia para la seguridad nacional.

Asimismo, ***el riesgo de perjuicio que supondría la divulgación de la información supera el interés general de que sea difundida****, en razón de que se busca proteger la estabilidad y soberanía del Estado Mexicano a través de la*

S4HrwykCIT99PZ1r51UQZihDV8v2kbcaKw0UylkHG3M=

protección a los sistemas e instrumentos que son utilizados en el desarrollo de sus funciones, con lo es su sistema de cómputo.

*Finalmente, se estima que la **limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo para evitar un posible perjuicio,** pues la reserva adoptada, constituye una medida de restricción temporal, la cual no es excesiva, en tanto que constituye una reserva temporal; máxime que el derecho a buscar y recibir información, si bien es un derecho fundamental, no es absoluto y puede ser limitado, siempre y cuando: i) el fin sea constitucionalmente válido (fin legitimo); ii) la medida sea idónea para alcanzar el fin constitucionalmente válido; iii) no exista un medio menos lesivo; y iv) la limitación sea proporcional en sentido estricto; como en este caso ocurre.*

Por lo anterior, es dable referir que, en principio procede la clasificación de la información requerida conforme al artículo 113, fracción I de la Ley General de Transparencia y Acceso a la Información Pública: sin embargo, debe precisarse que el solicitante requirió el tipo de contratación, empleo cargo o comisión de las personas físicas que cuentan con las contraseñas administrativas o su equivalente para el manejo, administración y control de la configuración de cada equipo de cómputo en las instalaciones de la Suprema Corte de Justicia de la Nación.

En ese sentido, este Instituto advierte que dicha información no da cuenta de las actividades operativas y logística encaminada a la preservación de la seguridad interior de la Federación, tampoco implica difundir la organización interna del sujeto obligado, de tal manera que no se prevé de qué manera la difusión de los datos en comento puedan comprometer la seguridad pública.

[...]

En razón de lo anterior, este Instituto, no advierte que se actualice la causal de reserva prevista en el numeral 113, fracción I de la Ley General de Transparencia y Acceso a la Información Pública, en relación con el tipo de contratación, empleo, cargo o comisión que desempeñen las personas que cuenten con las contraseñas administrativas o su equivalente.

Ahora bien, es pertinente señalar que, conforme a lo que dispone el artículo 65 de la Ley Federal de Transparencia y Acceso a la Información Pública, los Comités de Transparencia confirmarán, modificarán o revocarán las

S4HrwykCIT99PZ1r51UQZihDV8v2kbcaKw0UylkHG3M=

determinaciones en relación con la clasificación de información.

*Así, este Instituto estima que el agravio del particular, resulta **PARCIALMENTE FUNDADO**, por lo que se considera procedente **MODIFICAR** la respuesta de la Suprema Corte de Justicia de la Nación y se le **instruye** a efecto de que:*

- ✓ *Proporcione al recurrente el tipo de contratación, empleo, cargo o comisión de servidores públicos que cuenta con las contraseñas administrativas o su equivalente para el manejo, administración y control de la configuración de cada equipo de cómputo.*
- ✓ *Emita un acta debidamente fundada y motivada en la que clasifique la información como reservada de los siguientes puntos:*

1. Ordenado por 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.

2. Una relación de todos los puertos de red abiertos.

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

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

5. Nombre de las personas físicas que cuentan con las contraseñas administrativas o su equivalente (permisos informáticos, credenciales administrativas, privilegios de superusuario 'su', 'root', etc.) para el manejo, administración y control de la configuración de cada equipo.

7. 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.

8. El domicilio actual en donde se encuentra físicamente cada equipo.

Lo anterior, con fundamento en el artículo 110, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública, por un periodo de 05 años, debiendo aplicar la prueba de daño correspondiente.

En relación a lo anterior, y toda vez que en la solicitud de acceso se señaló como modalidad preferente: 'Plataforma Nacional de Transparencia', y ello ya no es posible, el sujeto obligado deberá entregar el acta antes referida al recurrente al medio que señaló para tales efectos o bien, ponerla a su disposición en un sitio de internet, y comunicar a este último los datos que le permitan acceder a la misma. […]

S4HrwykClT99PZ1r51UQZihDV8v2kbcaKw0UylkHG3M=

Por lo expuesto y fundado, el Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales:

RESUELVE

***PRIMERO**. Por las razones expuestas en el considerando Cuarto de la presente resolución, y con fundamento en lo que establece el artículo 157, fracción III de la Ley Federal de Transparencia y Acceso a la Información Pública, se **MODIFICA** la respuesta emitida por la Suprema Corte de Justicia de la Nación.*

***SEGUNDO**. Se instruye a la Suprema Corte de Justicia de la Nación para que, en un plazo no mayor de diez días hábiles, contados a partir del día hábil siguiente al de su notificación, cumpla con lo ordenado en la presente resolución e informe a este Instituto las acciones implementadas para tales efectos, de conformidad con lo dispuesto en el artículo 159, párrafo segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública. […]"*

IX. Resolución en cumplimiento a lo determinado por el INAI. El cinco de diciembre de dos mil diecisiete, este Comité de Transparencia determinó lo siguiente en el expediente CT-CUM-R/A-2-2018:

"A partir del contexto referido en el capítulo de antecedentes, este Comité de Transparencia atiende la resolución emitida por el Pleno del INAI en el recurso de revisión RRA 6063/18 y su acumulado RRA 6064/18.

En ese orden, importa hacer notar que en principio, el INAI en la determinación aludida, resolvió confirmar la clasificación de reserva de la información requerida que se menciona a continuación:

'1. Ordenado por Número de serie, de cada uno de los equipos de cómputo, y de cada uno de los MODEMS, ROUTERS (ruters) o Puntos de acceso inalámbricos, en posesión del sujeto obligado.

2. Una relación de todos los puertos de red abiertos.

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

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

5. Nombre de aquellas personas físicas que cuentan con las contraseñas administrativas o su equivalente (permisos informáticos, credenciales administrativas, privilegios de superusuario 'su', 'root', etc.) para el manejo, administración y control de la configuración de cada equipo.

S4HrwykCIT99PZ1r51UQZihDV8v2kbcaKw0UylkHG3M=

7. 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 DHCP.

8. El domicilio actual en donde se encuentra físicamente cada equipo.'

Lo anterior, al considerar que la divulgación de la información constituye un riesgo real, demostrable e identificable de perjuicio significativo al interés público, ya que se pudieran 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[2].

En ese contexto, ordenó a este Alto Tribunal, la emisión de un acta debidamente fundada y motivada en la que se clasifique como reservada dicha información, por un periodo de cinco años, aplicando la prueba de daño correspondiente.

Asimismo, por lo que hace a la reserva del tipo de contratación, empleo cargo o comisión de las personas físicas que cuentan con las contraseñas administrativas o su equivalente para el manejo, administración y control de la configuración de cada equipo de cómputo en las instalaciones de la Suprema Corte de Justicia de la Nación, ordenó modificar la clasificación de la información. Lo anterior, al estimar que dicha información: i) no da cuenta de las actividades operativas y logística encaminada a la preservación de la seguridad interior de la Federación; ii) tampoco implica difundir la organización interna del sujeto obligado; y iii) no se prevé de qué manera la difusión de los datos en comento puedan comprometer la seguridad pública.

Atento a ello, se solicitó a esta Suprema Corte de Justicia poner a disposición del peticionario la información en comento[3].

En ese orden, en aras de atender lo mandatado por el INAI, con fundamento en lo previsto en el artículo 113, fracción I, de la Ley General de Transparencia y Acceso a la Información Pública, se determina que la información requerida, aludida en el inciso a) anterior[4], es de carácter reservado.

---

[2] En términos del artículo 110, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública, que dispone:
'Artículo 110. *Conforme a lo dispuesto por el artículo 113 de la Ley General, 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; […]'*

[3] Esto es, *el tipo de contratación, empleo, cargo o comisión de servidores públicos que cuenta con las contraseñas administrativas o su equivalente para el manejo, administración y control de la configuración de cada equipo de cómputo.*

[4] Es decir, la información ordenada por *Número de serie, de cada uno de los equipos de cómputo, y de cada uno de los MODEMS, ROUTERS (ruters) o Puntos de acceso inalámbricos, en posesión del sujeto obligado, que se precisa a continuación:*

S4HrwykCIT99PZ1r51UQZihDV8v2kbcaKw0UylkHG3M=

Ello, atiende a que, como refiere la DGTI (área técnica) su divulgación pone en riesgo la información contenida en los equipos de este Alto Tribunal; quedando altamente vulnerables y sin protección[5].

Refuerza lo anterior, lo resuelto por el órgano garante en la determinación de treinta y uno de octubre de dos mil dieciocho, en la que estimó que la difusión de dicha información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público, ya que pudiera obstaculizar o bloquear las actividades de inteligencia o contrainteligencia y revelar normas, procedimientos, métodos, fuentes, especificaciones técnicas, tecnología o equipo que sean útiles para la generación de inteligencia para la seguridad nacional.

Es preciso señalar que lo anterior se actualiza también desde la especificidad que en la aplicación de la prueba de daño, disponen los artículos 103 y 104, de la Ley General de Transparencia, ya que, como se refirió, con la divulgación de la información que se analiza, se podrían identificar las tecnologías, esquemas de conectividad y de seguridad, que se emplean en la Suprema Corte para salvaguardar la información contenida en los sistemas de

---

- 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 aquellas personas físicas que cuentan con las contraseñas administrativas o su equivalente (permisos informáticos, credenciales administrativas, privilegios de superusuario 'su', 'root', etc.) 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 DHCP.
- El domicilio actual en donde se encuentra físicamente cada equipo.'

[5] *Lo anterior, al puntualizar que proporcionar cualquier dato o elemento que lleve a obtener información de acceso a los canales de comunicación de este Alto Tribunal puede:*
- Generar en sí un alto riesgo de vulnerabilidad, como lo sería: a) dar a conocer si se cuenta con cierto tipo de tecnología; b) el equipo que se usa; c) su ubicación; d) número de serie; e) marca; f) contraseñas; g) sitios; h) esquemas de conectividad y de seguridad; i) puertos abiertos; j) nombre de los programas informáticos de los firewall y conexiones de red IP; y k) los nombres de las personas físicas y los procedimientos que realizan para la operación, ya que todos estos elementos sirven para salvaguardar la información y comunicaciones que hacen uso del sistema de comunicaciones, y entregar alguno de ellos podrían poner en riesgo cuestiones de seguridad pública y con ello, el acceso a la justicia.
- Traer las siguientes consecuencias: a) 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; b) exponer 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; c) con la información requerida en su conjunto permitir que cualquier persona capacitada ingrese a los sistemas de comunicación y a la información que se aloje en estos sistemas; d) cualquier afectación al Alto Tribunal pondría de igual forma en riesgo a las otras instancias del Poder Judicial de la Federación.

S4HrwykCIT99PZ1r51UQZihDV8v2kbcaKw0UylkHG3M=

comunicaciones de este Alto Tribunal, poniendo en riesgo cuestiones de seguridad pública.

Lo anterior, se refuerza a partir de lo expuesto por el INAI en cuanto a que el riesgo que supondría la difusión de la información supera el interés general de que sea divulgada, en razón de que se busca proteger la estabilidad y soberanía del Estado Mexicano a través de la protección a los sistemas e instrumentos que son utilizados en el desarrollo de sus funciones, con lo es su sistema de cómputo.

En ese orden, y como pone de relieve el citado órgano garante, la limitación de la información se adecua al principio de proporcionalidad y representa el medio menos restrictivo para evitar un posible perjuicio, pues la reserva adoptada, constituye una medida de restricción temporal, la cual no es excesiva, en tanto que constituye una reserva temporal; máxime que el derecho a buscar y recibir información, si bien es un derecho fundamental, no es absoluto y puede ser limitado, siempre y cuando: i) el fin sea constitucionalmente válido (fin legitimo); ii) la medida sea idónea para alcanzar el fin constitucionalmente válido; iii) no exista un medio menos lesivo; y iv) la limitación sea proporcional en sentido estricto; como en este caso ocurre.

En virtud de lo expuesto, se confirma la clasificación de información reservada de los datos que se analizan, por un periodo de cinco años, en términos de lo previsto en los artículos 101, párrafo segundo y 113, fracción I de la Ley General de Transparencia y Acceso a la Información Pública[6].

Ahora bien, por lo que hace a la entrega de la información referida en el inciso b)[7], este órgano colegiado, de conformidad con lo establecido por el artículo 37 de los Lineamientos Temporales, estima necesario requerir respetuosamente a la Dirección General de Tecnologías de la Información[8], para que, en el plazo de dos días hábiles, en garantía del derecho de acceso a la información (el cual lleva aparejados los principios de eficacia y certeza), y tomando en

---

[6] '***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. […]'*
'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; […]'

[7] '***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*; […]'*

[8] *Lo anterior, tomando en cuenta que es el área encargada, entre otras cosas, de: a) administrar los recursos en materia de tecnologías de la información y comunicación y proveer los servicios que se requieran en la materia; b) proporcionar a la Dirección General de Presupuesto y Contabilidad la información presupuestal derivada del Programa Anual de Necesidades de Tecnologías de la Información, y c) ejecutar y actualizar los mecanismos de seguridad informática y vigilar su adecuado funcionamiento; ello, en términos de lo previsto por el artículo 27, fracciones I, III y XI, del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación.*

S4HrwykClT99PZ1r51UQZihDV8v2kbcaKw0UylkHG3M=

cuenta lo mandatado por el INAI[9], haga llegar la respuesta a la Unidad General de Transparencia y Sistematización de la Información Judicial.

De conformidad con lo dispuesto por los artículos 159, segundo párrafo, 169, primer párrafo, y 170, de la Ley Federal de Transparencia y Acceso a la Información Pública[10], la Unidad General de Transparencia deberá informar al INAI del cumplimiento de su resolución.

R E S U E L V E:

PRIMERO. *Se confirma la clasificación de reserva de los datos precisados en la presente resolución.*

SEGUNDO. *Se solicita a la Dirección General de Tecnologías de la Información para que atienda lo determinado en las consideraciones de esta resolución.*

TERCERO*. Se solicita a la Unidad General de Transparencia informe al Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales sobre el cumplimiento de su resolución.*

X. Requerimiento de datos para el índice de información reservada. Por oficio CT-218-2023 de veinticinco de mayo de dos mil veintitrés, la Secretaría de este Comité de Transparencia hizo del conocimiento a la Dirección General de Tecnologías de la Información lo siguiente:

"Con fundamento en el artículo 26, fracción XV, del Acuerdo General de Administración 05/2015, del tres de noviembre de dos mil quince, del Presidente de la Suprema Corte de Justicia de la Nación, por el que se expiden los lineamientos temporales para regular el procedimiento

---

9 *"**SEGUNDO**. **Se instruye a la Suprema Corte de Justicia de la Nación para que, en un plazo no mayor de diez días hábiles, contados a partir del día hábil siguiente al de su notificación, cumpla con lo ordenado en la presente resolución e informe a este Instituto las acciones implementadas para tales efectos**, de conformidad con lo dispuesto en el artículo 159, párrafo segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública*

10 '***Artículo 159***. *[…]*
Los sujetos obligados deberán informar al Instituto el cumplimiento de sus resoluciones en un plazo no mayor a tres días.
[…]
Artículo 169. *Los sujetos obligados, a través de la Unidad de Transparencia, darán estricto cumplimiento a las resoluciones del Instituto y deberán informar a estos sobre su cumplimiento.*
[…]
Artículo 170. *Transcurrido el plazo señalado en el artículo anterior, el sujeto obligado deberá informar al Instituto sobre el cumplimiento de la resolución y publicar en la Plataforma Nacional la información con la que se atendió a la misma."*

S4HrwykCIT99PZ1r51UQZihDV8v2kbcaKw0UylkHG3M=

administrativo interno de acceso a la información pública, así como el funcionamiento y atribuciones del Comité de Transparencia de la Suprema Corte de Justicia de la Nación le informo que el Comité de Transparencia, en sesión pública de 11 de enero de 2023, aprobó el índice de información reservada con corte a diciembre de 2022, el cual se elabora semestralmente y se registran únicamente aquellos asuntos cuya clasificación fue aprobada por el propio Comité de Transparencia (documento visible en el siguiente vínculo Información Clasificada | Suprema Corte de Justicia de la Nación (scjn.gob.mx).

En ese sentido, se hace de su conocimiento que, conforme a los registros del citado índice, se encuentra próximo a concluir el plazo de reserva de la información siguiente:

Número de registro	***Nombre del documento***	***Fecha de confirmación de clasificación del Comité de Transparencia***	***Fecha en que culmina el plazo de clasificación***
48	*Infraestructura*	*27/junio/2018 – expediente CT-CI/A-11-2018 y CT-CUM-R/A-2/2018 de 5/diciembre/2018*	*27 de junio de 2023*

En consecuencia, en virtud de que las personas titulares de las áreas son las responsables de clasificar la información y comunicar su vigencia al Comité de Transparencia, en términos del artículo 100, párrafo tercero de la Ley General de Transparencia y Acceso a la Información Pública, en relación con el numeral Trigésimo cuarto de los Lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, respetuosamente se solicita que, a más tardar el ***8 de junio de 2023****, informe sobre la vigencia de la referida información reservada bajo su resguardo, esto es,* ***si el plazo de la reserva es susceptible de ampliarse****, indicando las* ***razones y el fundamento legal*** *de esa condición, conforme lo disponen los artículos 101, párrafo tercero y 103, párrafo segundo, de la citada Ley General o, en su caso, si procede la* ***desclasificación (en tanto que hubieren dejado de subsistir las causas que dieron origen a la reserva).***

Es preciso aclarar que, en caso de desclasificarse, ello sería única y exclusivamente por lo que corresponde al supuesto de pronunciamiento plasmado en el registro, sin menoscabo que, para su difusión, por motivo de solicitud de información u otro mecanismo, sea necesario que el responsable se pronuncie sobre la pertinencia de elaborar versión pública o bien manifieste diversa circunstancia de reserva o impedimento de entrega. …”

XI. Presentación de informe. Mediante oficio DGTI/258/2023, de ocho de junio de dos mil veintitrés, la Dirección General de Tecnologías de la información manifestó lo siguiente:

S4HrwykCIT99PZ1r51UQZihDV8v2kbcaKw0UylkHG3M=

"Hago referencia al oficio número CT-218-2023, fechado el día 25 de mayo del año en curso, relativo a la actualización del índice de información reservada, a través del cual solicita se comunique sobre la vigencia del plazo de reserva del siguiente registro:

Número de registro	***Nombre del documento***	***Fecha de confirmación de clasificación del Comité de Transparencia***	***Fecha en que culmina el plazo de clasificación***
48	*Infraestructura*	*27/junio/2018 – expediente CT-CI/A-11-2018 y CT-CUM-R/A2/2018 de 5/diciembre/2018*	*27 de junio de 2023*

Al respecto se adjunta Atenta Nota de Cumplimiento, con números DGTI-SGIT-28-2023, DGTI-SGST-11-2023 y DGTI-DSI-13-2023, suscrita por el Ing. Francisco Alberto López Quiroz, Subdirector General de Infraestructura Tecnológica, el Ing. Francisco Javier Rojas Romero, Subdirector General de Servicios Tecnológicos, el Mtro. Omar Salinas García, Director de Seguridad Informática, el Lic. Javier Sánchez Valtierra, Director de Telecomunicaciones, el Mtro. José Eduardo Girón Camacho, Subdirector de Ciberseguridad, el Ing. Carlos Manuel Robles Mondragón, Director de Cómputo Personal, y el Ing. Luis Ángel Corro Ajungo, Subdirector de Comunicaciones Lógicas, mediante la cual emiten su pronunciamiento sobre el tema que nos ocupa.

[…]"

"ATENTA NOTA A LA DIRECTORA GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN.

ASUNTO: PRONUNCIAMIENTO SOBRE AMPLIACIÓN DE RESERVA

Me refiero al oficio número CT-218-2023, fechado el día 25 de mayo del año en curso, a través del cual hace del conocimiento que conforme a los registros del índice de información reservada con corte a diciembre de 2022, se encuentra próximo a concluir el plazo de reserva de la información del recurso de revisión CT-CUM-R/A-2-2018, derivado del diverso CT-CI/A-11-2018, por lo que solicita se informe si el plazo de la reserva es susceptible de ampliarse o si procede la desclasificación relacionado con:

> *'1. Ordenado por Número de serie, de cada uno de los equipos de cómputo, y de cada uno de los MODEMS, ROUTERS (ruters) o Puntos de acceso inalámbricos, en posesión del sujeto obligado.*
> *2. Una relación de todos los puertos de red abiertos.*
> *3. El nombre y versión del programa informático instalado para administrar o controlar lo referente al cortafuegos o firewall.*
> *4. Si se encuentra habilitada la conexión de red IPv6 (Protocolo de Internet versión 6).*
> *5. Nombre de aquellas personas físicas que cuentan con las contraseñas administrativas o su equivalente (permisos informáticos, credenciales administrativas, privilegios de superusuario 'su', 'root', etc.) para el manejo, administración y control de la configuración de cada equipo.*

S4HrwykCIT99PZ1r51UQZihDV8v2kbcaKw0UylkHG3M=

7. 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 DHCP.
8. El domicilio actual en donde se encuentra físicamente cada equipo.' (sic)

Al respecto y conforme al artículo 111 de la Ley Federal de Transparencia y Acceso a la Información Pública prevé que las causales de reserva previstas en el artículo 110 se deberán fundar y motivar, 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, mismo que 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 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.' (sic)

Bajo este contexto, debe señalarse que, la normativa establece las causales de reserva previstas a través de la aplicación de una prueba de daño que deben proporcionar los sujetos obligados, la cual para acreditarse debe cumplir con elementos que se señalan en el Trigésimo Tercero de los Lineamientos Generales antes mencionado.

Al divulgar la información que nos ocupa, se actualiza la siguiente prueba de daño:

➢ *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*

S4HrwykClT99PZ1r51UQZihDV8v2kbcaKw0UylkHG3M=

pudieran vulnerar la seguridad pública al haber riesgo en la intromisión no permitida.

➢ 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 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.

En conclusión, se actualiza la clasificación de la información solicitada, ya que subsisten las causas que dieron origen a su clasificación con fundamento en el artículo 113, fracción I de la Ley General de Transparencia y Acceso a la Información Pública y la fracción I del artículo 110 de la Ley Federal de Transparencia y Acceso a la Información Pública.

Ahora bien, en cuanto al periodo de reserva, el artículo 99 de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el Trigésimo Cuarto de los Lineamientos Generales, establecen que la información clasificada podrá permanecer con tal carácter, hasta por un periodo de cinco años, y que tal información podrá ser desclasificada: a) cuando se extingan las causas que dieron origen a su clasificación; b) cuando expire el plazo de clasificación; c) cuando exista resolución de una autoridad competente que determine que existe una causa de interés público que prevalece sobre la reserva de la información; d) cuando el Comité de Transparencia considere pertinente la desclasificación de conformidad con el Título

S4HrwykCIT99PZ1r51UQZihDV8v2kbcaKw0UylkHG3M=

cuarto del mismo ordenamiento, o e) cuando se trate de información que esté relacionada con violaciones graves a derechos humanos o delitos de lesa humanidad.

En el caso concreto, considerando que el bien jurídico tutelado es la seguridad pública, se considera que prevalecen las causas que originaron la reserva y por ello el periodo debe ampliarse.

Por último, todo lo anteriormente expuesto, se refuerza con lo resuelto por el Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) en sesión del treinta y uno de octubre de dos mil dieciocho, en el recurso de revisión RRA 6063/18 y su acumulado RRA 6064/18, en la cual resalta lo siguiente:

> *'…De lo anterior, se desprende que **el sujeto obligado argumentó que si bien existe un riesgo al difundir lo requerido**, ya que se podrían identificar las tecnologías, esquemas de conectividad y de seguridad, que se emplean en la Suprema Corte de Justicia de la Nación para salvaguardar la información contenida en los sistemas de comunicaciones de ese Alto Tribunal, poniendo en riesgo cuestiones de seguridad pública.*
>
> *En resumen, este Instituto considera que en el presente caso, **la divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público**, ya que pudiera obstaculizar o bloqueen las actividades de inteligencia o contrainteligencia y cuando se revelen normas, procedimientos, métodos, fuentes, especificaciones técnicas, tecnología o equipo que sean útiles para la generación de inteligencia para la seguridad nacional.*
>
> *Asimismo, **el riesgo de perjuicio que supondría la divulgación de la información supera el interés general de que sea difundida**, en razón de que se busca proteger la estabilidad y soberanía del Estado Mexicano a través de la protección a los sistemas e instrumentos que son utilizados en el desarrollo de sus funciones, como lo es su sistema de cómputo.*
>
> *Finalmente, se estima que **la limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo para evitar un posible perjuicio**, pues la reserva adoptada, constituye una medida de restricción temporal, la cual no es excesiva, en tanto que constituye una reserva temporal; máxime que el derecho a buscar y recibir información, si bien es un derecho fundamental, no es absoluto y puede ser limitado, siempre y cuando: i) el fin sea constitucionalmente válido (fin legitimo); ii) la medida sea idónea para alcanzar el fin constitucionalmente válido; iii) no exista un medio menos lesivo; y iv) la limitación sea proporcional en sentido estricto; como en este caso ocurre.*
>
> *Por lo anterior, es dable referir que, en principio procede la clasificación de la información requerida conforme al artículo 113, fracción I de la Ley General de Transparencia y Acceso a la Información Pública:' (SIC)*

Así como lo señalado por el Comité de Transparencia de la Suprema Corte de Justicia de la Nación, a través de la resolución del expediente CT-CUM-R/A-2/2018, derivado del diverso CT-CI/A-11-2018, que indica lo siguiente:

> *'…En ese orden, en aras de atender lo mandatado por el INAI, con fundamento en lo previsto en el artículo 113, fracción I, de la Ley General de Transparencia y Acceso a la Información Pública, se determina que la información requerida, aludida en el inciso a) anterior, es de carácter reservado. Ello, atiende a que,*

S4HrwykCIT99PZ1r51UQZihDV8v2kbcaKw0UylkHG3M=

como refiere la DGTI (área técnica) su divulgación pone en riesgo la información contenida en los equipos de este Alto Tribunal; quedando altamente vulnerables y sin protección.

Refuerza lo anterior, lo resuelto por el órgano garante en la determinación de treinta y uno de octubre de dos mil dieciocho, en la que estimó que la difusión de dicha información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público, ya que pudiera obstaculizar o bloquear las actividades de inteligencia o contrainteligencia y revelar normas, procedimientos, métodos, fuentes, especificaciones técnicas, tecnología o equipo que sean útiles para la generación de inteligencia para la seguridad nacional.

Es preciso señalar que lo anterior se actualiza también desde la especificidad que en la aplicación de la prueba de daño, disponen los artículos 103 y 104, de la Ley General de Transparencia, ya que, como se refirió, con la divulgación de la información que se analiza, se podrían identificar las tecnologías, esquemas de conectividad y de seguridad, que se emplean en la Suprema Corte para salvaguardar la información contenida en los sistemas de comunicaciones de este Alto Tribunal, poniendo en riesgo cuestiones de seguridad pública.

Lo anterior, se refuerza a partir de lo expuesto por el INAI en cuanto a que el riesgo que supondría la difusión de la información supera el interés general de que sea divulgada, en razón de que se busca proteger la estabilidad y soberanía del Estado Mexicano a través de la protección a los sistemas e instrumentos que son utilizados en el desarrollo de sus funciones, con lo es su sistema de cómputo.

En ese orden, y como pone de relieve el citado órgano garante, la limitación de la información se adecua al principio de proporcionalidad y representa el medio menos restrictivo para evitar un posible perjuicio, pues la reserva adoptada, constituye una medida de restricción temporal, la cual no es excesiva, en tanto que constituye una reserva temporal; máxime que el derecho a buscar y recibir información, si bien es un derecho fundamental, no es absoluto y puede ser limitado, siempre y cuando: i) el fin sea constitucionalmente válido (fin legitimo); ii) la medida sea idónea para alcanzar el fin constitucionalmente válido; iii) no exista un medio menos lesivo; y iv) la limitación sea proporcional en sentido estricto; como en este caso ocurre.

En virtud de lo expuesto, se confirma la clasificación de información reservada de los datos que se analizan, por un periodo de cinco años, en términos de lo previsto en los artículos 101, párrafo segundo y 113, fracción I de la Ley General de Transparencia y Acceso a la Información Pública.' (sic)."

XII. Acuerdo de turno. Mediante acuerdo de nueve de junio de dos mil veintitrés, la Presidencia del Comité de Transparencia de este Alto Tribunal ordenó integrar el expediente CT-CUM/A-20-2023 que fue remitido al Titular de la Unidad General de Investigación de Responsabilidades Administrativas, en su carácter de

S4HrwykCIT99PZ1r51UQZihDV8v2kbcaKw0UylkHG3M=

integrante de dicho órgano, para que conforme a sus atribuciones procediera al estudio y propuesta de resolución respectiva, en términos de lo dispuesto en los artículos 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública (Ley General), y 23, fracción II, y 27 del Acuerdo General de Administración 5/2015.

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

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

II. Análisis de ampliación de reserva. Como se advierte en el antecedente I, en la solicitud que da origen al presente asunto, se pidió la información que se precisa a continuación sobre los módems, *routers* y puntos de acceso a internet inalámbrico de la Suprema Corte de Justicia de la Nación

- Una relación de todos los puertos de red abiertos.
- Nombre y versión del programa informático instalado para administrar o controlar lo referente al cortafuegos o *firewall* (en inglés).
- Si se encuentra habilitada la conexión de red IPv6 (protocolo de Internet versión 6).
- Nombre de aquellas personas físicas que cuentan con las contraseñas administrativas o su equivalente (permisos informáticos, credenciales administrativas, privilegios de superusuario *'su' 'root'*, etc.) para el manejo, administración y control de la configuración de cada equipo. Tipo de contratación, empleo, cargo o comisión que desempeñan las personas que resultan de la lista de todos los puntos de red abiertos.

S4HrwykClT99PZ1r51UQZihDV8v2kbcaKw0UylkHG3M=

- 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 DHCP, por sus siglas en inglés *Dynamic Host Configuration Protocol*).
- Domicilio actual en que se encuentra físicamente cada equipo.

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-5-2018[11] en el cual se validó que la documentación relacionada

[11] "*(…) Ahora bien, para sustentar la reserva, la Dirección General de Tecnologías de la Información manifestó substancialmente, lo siguiente:*

- *Dar a conocer si se cuenta con* ***cierto tipo de tecnologías, su ubicación, números de serie, marca, contraseñas, sitios, esquemas de conectividad y de seguridad, así como equipos que se usan para salvaguardar la información y comunicaciones que hacen uso del sistema de comunicaciones del Alto Tribunal,*** *pone en riesgo cuestiones de seguridad púbica y, con ello, el acceso a la justicia.*

(…) este Comité advierte que según se precisó, otorgar la información solicitada podría exponer la capacidad de reacción ante posibles ataques cibernéticos, (…).

Así, ***la motivación que otorga el área y considerando que se trata de un área técnica que conforme a sus atribuciones es responsable del manejo de esos equipos, se arriba a la conclusión que sobre la información requerida pesa la reserva establecida en la fracción I, del artículo 113, de la Ley General,*** *que establece (…)*

Se afirma que se actualiza esa hipótesis, porque se podría comprometer un aspecto de la seguridad pública en general, ya que, se reitera, 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 de vulnerabilidad ante un ataque cibernético y suplantación de identidad.

(…) 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.

De igual manera, como se mencionó en la citada resolución CT-CI/A-3-2018, este Comité de Transparencia identifica que se pretende proteger, desde un esquema global, los sistemas de comunicaciones del Alto Tribunal, en el caso concreto, lo que implica el acceso a la red inalámbrica, en tanto que se podrán involucrar negativamente aspectos de seguridad pública

S4HrwykCIT99PZ1r51UQZihDV8v2kbcaKw0UylkHG3M=

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[12].

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:

1. Confirmar la reserva de la información solicitada en lo que hace a:

---

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 cibernético y suplantación de identidad.

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.”*
[Lo resaltado es propio].

[12] “***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 correará a partir de la fecha en que se clasifique el documento…”

S4HrwykClT99PZ1r51UQZihDV8v2kbcaKw0UylkHG3M=

- 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) 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.

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.

2. por lo que hace a la información del *tipo de contratación, empleo, cargo o comisión de las personas físicas que cuentan con las contraseñas administrativas o su equivalente para el manejo, administración y control de la configuración de cada equipo de cómputo en las instalaciones de la Suprema Corte de Justicia de la Nación,* ordenó modificar la clasificación de la información; por considerar que dicha información i) no da cuenta de las

S4HrwykCIT99PZ1r51UQZihDV8v2kbcaKw0UylkHG3M=

actividades operativas y logísticas encaminadas a la preservación de la seguridad interna de la Federación, ii) tampoco implica difundir la organización interna del sujeto obligado, y iii) no se prevé de qué manera la difusión de los datos en comento puedan comprometer la seguridad pública.

De conformidad con lo anterior, en cumplimiento a la resolución emitida por el Pleno del INAI, este órgano colegiado determinó poner a disposición de la persona solicitante la información previamente referida en el punto 2 y confirmar la clasificación de lo señalado en el punto **1** de conformidad con lo siguiente:

- Atendiendo a lo referido por la DGTI (área técnica) su divulgación pone en riesgo la información contenida en los equipos de este Alto Tribunal, quedando altamente vulnerable y sin protección.
- La difusión de dicha información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público, ya que pudiera obstaculizar o bloquear las actividades de inteligencia o contrainteligencia y revelar normas, procedimientos o métodos, fuentes, especificaciones técnicas, tecnología o equipo que sean útiles para la generación de inteligencia para la seguridad nacional.
- Específicamente en la aplicación de la prueba de daño dispuesta en los artículos 103 y 104, de la Ley General de Transparencia, se determinó que con la divulgación de la información que se analiza, se podrían identificar las tecnologías, esquemas de conectividad y de seguridad, que se emplean en la Suprema Corte para salvaguardar la información contenida en los sistemas de comunicaciones de este Alto Tribunal, poniendo en riesgo cuestiones de seguridad pública.
- Lo anterior reforzado por lo expuesto por el INAI en cuanto a que supera el interés general de que sea divulgada, en razón de que se busca proteger la estabilidad y soberanía del Estado Mexicano a través de la protección a los sistemas e instrumentos que son utilizados en el desarrollo de sus funciones, con lo es su sistema de cómputo.
- La limitación de la información se adecua al principio de proporcionalidad y representa el medio menos restrictivo para evitar

S4HrwykClT99PZ1r51UQZihDV8v2kbcaKw0UylkHG3M=

> un posible perjuicio, pues la reserva adoptada, constituye una medida de restricción temporal, la cual no es excesiva, en tanto que constituye una reserva temporal; máxime que el derecho a buscar y recibir información, si bien es un derecho fundamental, no es absoluto y puede ser limitado, siempre y cuando: i) el fin sea constitucionalmente válido (fin legitimo); ii) la medida sea idónea para alcanzar el fin constitucionalmente válido; iii) no exista un medio menos lesivo; y iv) la limitación sea proporcional en sentido estricto; como en este caso ocurre.

Ahora, ya que el plazo de reserva de la información está próximo a concluir[13], 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.

Por lo que dicha instancia pone a consideración de este Comité la ampliación del plazo de reserva por cinco años.

Para analizar lo propuesto por la Dirección General de Tecnologías de la Información, se tiene presente que en términos del artículo 100, último párrafo de la Ley General de Transparencia[14], en relación con el diverso 17, párrafo primero, del

[13] 27 de junio de 2023, teniendo en cuenta que en resolución de 27 de junio de 2018 se confirmó la clasificación de la información.
[14] “***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.”

S4HrwykCIT99PZ1r51UQZihDV8v2kbcaKw0UylkHG3M=

Acuerdo General de Administración 5/2015[15], los titulares de las instancias que tienen bajo resguardo la información requerida son responsables de determinar su disponibilidad y clasificarla conforme a la normativa aplicable.

En ese sentido, en términos del artículo 36, fracciones I y IV del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación[16], la Dirección General Tecnologías de la Información tiene entre sus atribuciones administrar los recursos, proponer las políticas y lineamientos en materia de tecnologías de la información y comunicación, así como proveer los servicios que se requieren en la materia, planificar, diseñar, desarrollar y mantener en operación los sistemas informáticos jurídicos, administrativos y jurisdiccionales.

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

S4HrwykClT99PZ1r51UQZihDV8v2kbcaKw0UylkHG3M=

---

[15] *"**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.
(…)"

[16] *"**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;*
(…)
***IV.** Proponer al Oficial Mayor las políticas y lineamientos en materia de tecnologías de la información y comunicación para la Suprema Corte;*
***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;…"*

información 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.

c) 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.

El área vinculada refuerza lo expuesto, con lo determinado en las resoluciones de este Comité de Transparencia en los expedientes CT-CI/A-5-2018 y CT-CI/A-3-2018.

S4HrwykCIT99PZ1r51UQZihDV8v2kbcaKw0UylkHG3M=

Ello en virtud de que, la DGTI al realizar la prueba de daño argumentó que existe un riesgo real, demostrable e identificable de perjuicio significativo al interés público, toda vez que la difusión de lo requerido conllevaría a la Suprema Corte de Justicia de la Nación se podrían revelar especificaciones técnicas de los equipos, conexiones y programas que pudieran vulnerar la seguridad pública al haber riesgo en la intromisión no permitida.

Agregó que el riesgo de perjuicio que podría producirse con la publicidad de la información superaría el interés público general de conocerla; toda vez que, la divulgación de la información daría lugar a la suplantación de identidad para acceder a la red o 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, y se expondría la capacidad de la red ante posibles ataques informáticos porque se identificaría o remitiría información contenida en los equipos, servidores, equipos de comunicación, lo que atentaría contra la seguridad y conectividad tecnológica que se tiene implementada.

Además de que se pondría en riesgo a 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 este Alto Tribunal interconecta con los demás órganos del Poder Judicial.

Sumado a que se expondría la capacidad de reacción de la Suprema Corte de Justicia de la Nación ante posibles ataques cibernéticos, con lo cual se comprometería uno de los aspectos de la seguridad pública en general.

En ese sentido la DGTI precisa que la clasificación de la información 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, porque su divulgación implicaría el acceso a inteligencia o contrainteligencia y se revelarían normas, equipos, procedimientos, métodos, fuentes, especificaciones técnicas, tecnología o equipo.

S4HrwykClT99PZ1r51UQZihDV8v2kbcaKw0UylkHG3M=

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, respecto de la siguiente información:

- Número de serie, de cada uno de los equipos de cómputo, y de cada uno de los *MODEMS*, *ROUTERS* (rúters) 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 aquellas personas físicas que cuentan con las contraseñas administrativas o su equivalente (permisos informáticos, credenciales administrativas, privilegios de superusuario *“su”, “root”,* etc.) 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 DHCP*.
- El domicilio actual en donde se encuentra físicamente cada equipo.

S4HrwykClT99PZ1r51UQZihDV8v2kbcaKw0UylkHG3M=

Ahora, respecto del plazo, 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 cual, 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 que dieron origen a su clasificación.

Por lo expuesto y fundado; se,

R E S U E L V E:

ÚNICO. Se autoriza la ampliación de reserva de la información materia de análisis de la presente resolución.

Notifíquese a la instancia vinculada, así como a la Unidad General de Transparencia y Sistematización de Información Judicial y, en su oportunidad, archívese como asunto concluido.

Así, por unanimidad de votos, lo resolvió el Comité de Transparencia de la Suprema Corte de Justicia de la Nación y firman el Licenciado Mario José Pereira Meléndez, Director General de Asuntos Jurídicos y Presidente del Comité; el Maestro Christian Heberto Cymet López Suárez, Contralor del Alto Tribunal, y el Licenciado Adrián González Utusástegui, Titular de la Unidad General de Investigación de Responsabilidades Administrativas; integrantes del Comité, ante la Secretaria del Comité, quien autoriza y da fe.

LICENCIADO MARIO JOSÉ PEREIRA MELÉNDEZ
PRESIDENTE DEL COMITÉ

MAESTRO CHRISTIAN HEBERTO CYMET LÓPEZ SUÁREZ
INTEGRANTE DEL COMITÉ

S4HrwykClT99PZ1r51UQZihDV8v2kbcaKw0UylkHG3M=

LICENCIADO ADRIÁN GONZÁLEZ UTUSÁSTEGUI
INTEGRANTE DEL COMITÉ

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."

AGU/kmo

S4HrwykCIT99PZ1r51UQZihDV8v2kbcaKw0UylkHG3M=