RECURSO DE REVISIÓN CT-CUM-R/A-2-2018, derivado del diverso CT-CI/A-11-2018

ÁREA 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 cinco de diciembre de dos mil diecisiete.

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

I. Solicitud de información con folio 0330000106518. El diecisiete de mayo de dos mil dieciocho, se recibió en la Plataforma Nacional de Transparencia la solicitud referida, a través de la cual se requirió lo siguiente:

> "[…] 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 (ruters) 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 ingles). 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 DISTYRITO" [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 (Unidad General de Transparencia), solicitó al peticionario que precisara el tipo

de documento e instancia del amparo indirecto aludido en su solicitud, y qué es lo que concretamente requería de dicho expediente.

III. Desahogo de la prevención de la solicitud con folio 0330000106518. El veintinueve de mayo de dos mil dieciocho, el peticionario 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. 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 ingles). 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." [sic.]

IV. Solicitud de información con folio 0330000114618. El treinta de mayo de dos mil dieciocho, se recibió en la Plataforma Nacional de Transparencia la solicitud aludida, a través de la cual se requirió lo siguiente:

> "[…] 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 (ruters) 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 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 ingles Dynamic Host Configuration Protocol). d. Domicilio actual en donde se encuentra físicamente cada equipo." [sic.]

V. Respuestas de la Unidad de Transparencia. El diez de julio de dos mil dieciocho, la Unidad General de Transparencia respondió las solicitudes de información **0330000106518** y **0330000114618**, adjuntando la determinación de fecha veintisiete de junio de dos mil dieciocho, a través de la cual -a partir de lo señalado por la Dirección General de Tecnologías de la Información (DGTI)[1], en cuanto a que dar a conocer los datos requeridos pondría en riesgo cuestiones de seguridad pública y con ello, el acceso a la justicia-, este órgano colegiado confirmó la clasificación de reserva de la información requerida[2].

VI. Interposición y trámite de los recursos de revisión.

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

b) Mediante acuerdo de siete de septiembre de dos mil dieciocho, el INAI admitió a trámite el recurso de revisión interpuesto en contra de la respuesta dada por la Unidad General de Transparencia, a la solicitud de información **0330000114618**, mismo que quedó registrado

---

[1] Área que cuenta con el personal especializado para velar por la seguridad de la información contenida en los sistemas tecnológicos de la Suprema Corte.

[2] Información *ordenada 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*, que se precisa a continuación: i) una relación de todos los puertos de red abiertos; ii) el nombre y versión del programa informático instalado para administrar o controlar lo referente al cortafuegos o firewall (en ingles); iii) si se encuentra habilitada la conexión de red IPv6 (Protocolo de Internet versión 6). ; iv) el 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; v) **Tipo de contratación, empleo, cargo o comisión que desempeñan las personas que resultan del inciso a**. vi) 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 ingles Dynamic Host Configuration Protocol); vi) domicilio actual en donde se encuentra físicamente cada equipo.”

bajo el número RRA 6064/18, bajo la ponencia del Comisionado Joel Salas Juárez.

c) Por acuerdo de once de septiembre de dos mil dieciocho, el INAI admitió a trámite el diverso recurso de revisión promovido contra la respuesta efectuada por la Unidad General de Transparencia, a la solicitud de información **0330000106518**, el cual quedó registrado bajo el número RRA 6063/18, bajo la ponencia del Comisionado Rosendoevgueni Monterrey Chepov.

d) Mediante acuerdo de veintiséis de septiembre del presente año, el INAI determinó la acumulación de los expedientes aludidos, agregándose los asuntos del recurso identificado como RRA 6064/18 al diverso expediente número RRA 6063/18, bajo la ponencia del Comisionado Rosendoevgueni Monterrey Chepov.

VII. Resolución del recurso de revisión. El Pleno del INAI en sesión de treinta y uno de octubre de dos mil dieciocho emitió resolución, en la cual, en la parte que nos ocupa, determinó lo siguiente:[3]

> *"[…]*
> *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.*
>
> *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****.*

[3] Expediente UE-A/0120/2016. Fojas170 a 229.

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 presentar las siguientes consecuencias:*

  - ✓ *La suplantación de identidad para acceder a la red y a toda la infraestructura tecnológica y de comunicaciones, con lo que podría extraerse información sobre la conducción de los expedientes judiciales o procedimientos administrativos seguidos en forma de juicio que no hayan causado estado.*
  - ✓ *Se 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 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 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 (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 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. […]*
>
> *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.* […]"
> [sic.]

VIII. Remisión del expediente a la Secretaría del Comité de Transparencia. Mediante oficio UGTSIJ/TAIPDP/3313/2016, recibido el treinta de noviembre de dos mil dieciocho, en la Secretaria de este órgano colegiado, el Titular de la Unidad General de Transparencia informó al Comité de Transparencia la resolución emitida por el Pleno del INAI, anexando el expediente formado con motivo de la solicitud de origen, para que en su caso, se determinen las acciones correspondientes para dar cumplimiento a la determinación en comento.

IX. Acuerdo de turno. Con esa misma fecha, el Presidente del Comité de Transparencia de este Alto Tribunal, ordenó integrar el expediente **CT-CUM-R/A-2-2018**, y turnar el asunto al Titular de la Unidad General de Enlace con los Poderes Federales de esta Suprema Corte de Justicia de la Nación, en su carácter de integrante del mismo, a efecto de elaborar el proyecto de resolución que cumplimente la resolución emitida por el Pleno del INAI.

X. Seguimiento del proyecto. En sesión del día de hoy, ante la ausencia del Titular de la Unidad General de Enlace con los Poderes Federales en la sesión, el Secretario Jurídico de la Presidencia hizo suyo el presente proyecto de resolución.

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

Este Comité de Transparencia de la Suprema Corte de Justicia de la Nación es competente para conocer y resolver el presente asunto, con fundamento en los artículos 1° y 6º de la Constitución Política de los Estados Unidos Mexicanos; 44, fracciones I y II, 113, fracción V, 151, párrafo segundo, 153, párrafo segundo, 196 y 197, de la Ley General de Transparencia y Acceso a la Información Pública; y 65, fracciones I y II, 110, fracción V, 157, párrafo segundo, 159, párrafo segundo, 163, párrafo primero, 168, 169 y 170, párrafo primero, de la Ley Federal de Transparencia y Acceso a la Información Pública; así como 23, fracciones I y II, y 27, del ACUERDO GENERAL DE ADMINISTRACIÓN 05/2015, DEL PRESIDENTE DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN, POR EL QUE SE EXPIDEN 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 (LINEAMIENTOS TEMPORALES).[4]

[4] Publicado en el Diario Oficial de la Federación el diez de noviembre de dos mil quince.

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.*
>
> *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[5].

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[6]*.*

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)

---

[5] 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; […]"

[6] 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.*

anterior[7], es de carácter reservado. 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[8].

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*

---

[7] Es decir, l*a 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:*
- *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."*

[8] 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.

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[9].

Ahora bien, por lo que hace a la entrega de la información referida en el inciso b)[10], 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[11], 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 cuenta lo mandatado por el INAI[12], 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,[13] la Unidad General de

---

[9] **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**; […]"

[10] Consistente en *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*.

[11] 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.

[12] "***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.*

[13] "**Artículo 159.** […]

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.

Notifíquese al Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, al solicitante, a la Unidad General de Transparencia y Sistematización de la Información Judicial y a las áreas vinculadas, y en su oportunidad, archívese como asunto concluido.

Así, por unanimidad de dos votos, lo resolvió el Comité de Transparencia de la Suprema Corte de Justicia de la Nación; y firman los licenciados Alejandro Manuel González García,

---

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."
[…]

Secretario Jurídico de la Presidencia, Presidente y Juan Claudio Delgado Ortiz Mena, Contralor del Máximo Tribunal, integrantes del Comité, ante el Secretario del mismo, que autoriza y da fe.

LICENCIADO ALEJANDRO MANUEL GONZÁLEZ GARCÍA
PRESIDENTE DEL COMITÉ

LICENCIADO JUAN CLAUDIO DELGADO ORTIZ MENA
INTEGRANTE DEL COMITÉ

LICENCIADO LUIS RAMÓN FUENTES MUÑOZ
SECRETARIO DEL COMITÉ

Esta hoja corresponde a la última del expediente CT-CUM-R/A-2/2018, emitida por el Comité de Transparencia de la Suprema Corte de Justicia de la Nación, en sesión de cinco de diciembre de dos mil dieciocho. CONSTE.-