CLASIFICACIÓN DE INFORMACIÓN CT-CI/A-11-2018
Derivado de los diversos UT-A/0190/2018 y UT-A/0200/2018

INSTANCIA REQUERIDA:

- **DIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN.**

Ciudad de México. Resolución del Comité de Transparencia de la Suprema Corte de Justicia de la Nación, correspondiente al veintisiete de junio de dos mil dieciocho.

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, 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."*

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."*

V. Acuerdo de admisión de la solicitud. El treinta de mayo de dos mil dieciocho, el Subdirector General de la Unidad General de

Transparencia y Sistematización de la Información Judicial, una vez analizada la naturaleza y contenido de las solicitudes, las estimó procedentes y ordenó abrir los expedientes UT-A/0198/2018 y UT-A/0200/2018.

VI. Requerimiento de información. El Titular de la Unidad General de Transparencia y Sistematización de la Información Judicial a través de los oficios UGTSIJ/TAIPDP/1661/2018 y UGTSIJ/TAIPDP/1659/2018, de treinta y treinta y uno, ambos de mayo de dos mil dieciocho, respectivamente, solicitó a la Dirección General de Tecnologías de la Información que se pronunciara sobre la existencia y clasificación de la información materia de las solicitudes.

VII. Respuesta del área requerida. La Dirección General de Seguridad, a través del oficio DGTI/DAPTI-1176-2018, de cuatro de junio de dos mil dieciocho, en atención a las solicitudes de referencia, informó lo siguiente:

> *"[…]* ***Respuestas:***
>
> *Primeramente es importante resaltar, que proporcionar cualquier dato o elemento que lleve a obtener información de acceso a los canales de comunicación de este Alto Tribunal, generan en sí un alto riesgo de vulnerabilidad, algunos de estos elementos pueden ser el dar a conocer si se cuenta con cierto tipo de tecnología, el equipo que se usa, su ubicación, número de serie, marca, contraseñas, sitios, esquemas de conectividad y de seguridad, puertos abiertos, nombre de los programas informáticos de los firewall y conexiones de red IP, así como 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 del Alto Tribunal, y proporcionar alguno de ellos podrían poner en riesgo cuestiones de seguridad pública y con ello, el acceso a la justicia.*
> *Asimismo, se pueden tener las siguientes consecuencias:*
>
> - *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.*

- *Cualquier afectación al Alto Tribunal pondría de igual forma en riesgo a las otras instancias del PJF, teniendo como una cuestión de seguridad pública tanto para el PJF, como para los justiciables; ya que la red de comunicaciones de la SCJN, interconecta con los demás órganos del Poder Judicial de la Federación (CJF, Juzgados de Distrito, Tribunales Unitarios, Tribunales Colegiados y TEPJF).*

Adicional a todo lo anterior, se identifica que este tipo de información está directamente relacionada a solicitudes previas, las cuales por las razones antes expuestas se clasificaron como reservadas. Los expedientes de clasificación con los que se identifican son:

- *CT-CI/A-3-2018 de la Octava Sesión Pública Ordinaria celebrada el dieciocho de abril del año en curso.*
- *CT-CI/A-5-2018 de la Novena Sesión Pública Ordinaria celebrada el dos de mayo del año en curso.*

Por lo anterior, la información solicitada es clasificada como reservada, con fundamento en la Ley General de Transparencia y Acceso a la Información Pública, en el artículo 113, fracción I; ya que son datos que deben tratarse con mucha cautela y no pueden proporcionarse, debido a que ponen en riesgo la información contenida en los equipos de este alto Tribunal; quedando altamente vulnerables y sin protección. […]"

VIII. Remisión del expediente. El ocho de junio de dos mil dieciocho el Titular de la Unidad General de Transparencia y Sistematización de la Información Judicial, a través de los oficios UGTSIJ/TAIPDP/1735/2018 y UGTSIJ/TAIPDP/1736/2018, remitió los expedientes UT-A/0198/2018 y UT-A/0200/2018 a la Secretaría del Comité de Transparencia, correspondientemente, con la finalidad de que se dictara la resolución de mérito.

IX. Acuerdo de turno y acumulación. Mediante acuerdo de once de junio de dos mil dieciocho, el Presidente del Comité de Transparencia de este Alto Tribunal ordenó acumular las solicitudes de referencia e integrar el expediente CT-CI/A-11-2018 y lo turnó al Titular de la Unidad General de Enlace con los Poderes Federales, para que procediera al estudio y propuesta de resolución respectiva.

X. Prórroga. En sesión de trece de junio de dos mil dieciocho, el Comité de Transparencia autorizó la ampliación del plazo extraordinario para atender lo concerniente a las solicitudes que nos ocupan.

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

PRIMERA. Competencia. El Comité de Transparencia de la Suprema Corte de Justicia de la Nación es competente para conocer y resolver el presente asunto, en términos de lo dispuesto en los artículos 6°, de la Constitución Política de los Estados Unidos Mexicanos, 4 y 44, fracciones I y II, de la Ley General de Transparencia y Acceso a la Información Pública, 65, fracciones I y II, de la Ley Federal de Transparencia y Acceso a la Información Pública, así como 23, fracciones II y III, del Acuerdo General de Administración 5/2015.

SEGUNDA. 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 registre el ejercicio de sus atribuciones, en términos de las leyes General 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 modems, 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 ingles).*
- *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 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).*
- *Domicilio actual en donde se encuentra físicamente cada equipo."*

En respuesta, el Director General de Seguridad 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 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.*

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[1], validó la clasificación

---

[1] "[…] 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 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 y comunicaciones que hacen uso del sistema de comunicaciones del Alto Tribunal**, pone en riesgo cuestiones de seguridad pública 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 del 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 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 podrían involucrar negativamente aspectos de seguridad pública que inciden directamente en su tarea sustantiva, ya que se podría acceder a la información inmersa en dichos equipos y con ello, se reitera, potencializar el nivel de vulnerabilidad de un ataque 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."

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 partir del uso del número de serie o de parte de los *modems*, *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 de seguridad pública y con ello, el acceso a la justicia, 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*[2]*;* este órgano colegiado procede a confirmar la reserva.

Lo anterior se actualiza también 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

---

[2] *En tanto que cualquier persona capacitada pudiera ingresar a los sistemas de comunicación y a la información que se aloje en dichos sistemas; pudiéndose extraer información sobre la conducción de los expedientes judiciales o procedimientos administrativos seguidos en forma de juicio que no hayan causado estado y exponer la capacidad de la red ante posibles ataques informáticos.*

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,

R E S U E L V E:

ÚNICO. Se confirma la clasificación de reserva efectuada por la Dirección General de Tecnologías de la Información, en los términos de esta determinación.

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

Por unanimidad de votos lo resolvió el Comité de Transparencia de la Suprema Corte de Justicia de la Nación, integrado por el licenciado Alejandro Manuel González García, Secretario Jurídico de la Presidencia y Presidente del Comité, Magistrado Constancio Carrasco Daza, titular de la Unidad General de Enlace con los Poderes Federales y licenciado Juan Claudio Delgado Ortiz Mena, Contralor del Alto Tribunal; quienes firman con el secretario del Comité que autoriza.

LICENCIADO ALEJANDRO MANUEL GONZÁLEZ GARCÍA
PRESIDENTE DEL COMITÉ

MAGISTRADO CONSTANCIO CARRASCO DAZA
INTEGRANTE DEL COMITÉ

LICENCIADO JUAN CLAUDIO DELGADO ORTIZ MENA
INTEGRANTE DEL COMITÉ

LICENCIADO LUIS RAMÓN FUENTES MUÑOZ
SECRETARIO DEL COMITÉ