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

CLASIFICACIÓN DE INFORMACIÓN
CT-CI/A-2-2021

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 enero de dos mil veintiuno.

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

I. Solicitud de información. El cuatro de enero de dos mil veintiuno, se recibió la solicitud tramitada en la Plataforma Nacional de Transparencia con el folio 0330000000221, requiriendo:

> *"Con base en mi derecho a la información y en versión pública, solicito conocer el número total de ataques cibernéticos que registró la institución, del 1 de enero de 2020 a la fecha. Favor de detallar por ataques totales, tipo de ataque, país de procedencia, tipo de afectación y si se levantó alguna denuncia penal, y en su caso, si hubo algún detenido."*

II. Acuerdo de admisión de la solicitud. En acuerdo de cinco de enero de dos mil veintiuno, la Unidad General de Transparencia y Sistematización de la Información Judicial, por conducto de su Subdirector General, una vez analizada la naturaleza y contenido de la solicitud, con fundamento en los artículos 123 y 124, de la Ley General de Transparencia y Acceso a la Información Pública, 124 y 125, de la Ley Federal de Transparencia y Acceso a la Información Pública y 7 del

Acuerdo General de Administración 5/2015, la estimó procedente y ordenó abrir el expediente UT-A/0002/2021.

III. Requerimiento de información. El Titular de la Unidad General de Transparencia y Sistematización de la Información Judicial, a través del oficio UGTSIJ/TAIPDP/0002/2021, enviado mediante comunicación electrónica de seis de enero de dos mil veintiuno, solicitó a la Dirección General de Tecnologías de la Información que se pronunciara sobre la existencia y clasificación de la información materia de la solicitud.

IV. Informe de la Dirección General de Tecnologías de la Información. El trece de enero de dos mil veintiuno, se recibió en la cuenta de correo electrónico habilitada para tales efectos por la Unidad General de Transparencia, el oficio DGTI/24/2021 digitalizado, en el que la titular de esa dirección general señala que remite la Atenta Nota DGTI-DSI-01/2021 en la que el Director de Seguridad Informática y el Jefe de Departamento de Criptografía y Autentificación dan respuesta a lo requerido en la solicitud, la cual se transcribe enseguida:

> *"Al respecto le informó que en el periodo del ejercicio de 2020 al día 7 de enero del año en curso, la Suprema Corte de Justicia de la Nación recibió 1,234 intentos de ataques cibernéticos, de acuerdo con el siguiente detalle:*

Periodo	***Total***
ene-20	*52*
feb-20	*111*
mar-20	*141*
abr-20	*149*
may-20	*171*
jun-20	*105*
jul-20	*99*
ago-20	*74*
sep-20	*79*
oct-20	*99*
nov-20	*78*
dic-20	*67*

ene-21	*9*
TOTAL	***1,234***

Ahora bien, por lo que respecta a la información sobre el tipo y lugar de origen, hago de su conocimiento que la misma se encuentra reservada; lo anterior, de conformidad con lo establecido en la resolución correspondiente al expediente de Cumplimiento CT-CUM/A-36-2018, que a la letra dice:

> *"Diariamente a nivel mundial se registran miles de ataques informáticos dirigidos a realizar fraudes, generar denegación de servicios, distribución de códigos maliciosos, así como llevar a cabo el robo de información particular de Instituciones del sector público, privado y ciudadanos en general. - - - La ciberdelincuencia se encarga de hacer uso de diferentes herramientas y técnicas con la finalidad de obtener información que les permita acceder a los sistemas de cómputo de Instituciones públicas, privadas y personas físicas para realizar un ataque informático en contra de ellos. La información sensible que buscan es: claves de acceso, paswords, direcciones OP, tipos de sistemas, tipos de herramientas de seguridad informática, etc. - - - En la actualidad, una de las principales técnicas para obtener información es conocida como "Ingeniería Social", la cual consiste en el uso de habilidades sociales de forma consiente y muchas veces premeditada para obtener información sensible. Para el caso de sector público, a través de solicitudes de acceso a la información, se puede solicitar y en su caso proporcionar información sensible que pueda facilitar a la ciberdelincuencia un ataque contra los sistemas gubernamentales. - - - Cada pieza de información que sea proporcionada a un hacker haciéndose pasar por un ciudadano, aumenta el nivel de riesgos de cualquier plataforma informática, ya que mediante el uso de técnicas de hackeo dirigidas denominadas "exploits", aprovechan las vulnerabilidades informáticas presentes en los sistemas, los cuales son fáciles de identificar al contar con información del sistema informático al cual se desea atacar, como puede ser el tipo de sistema operativo, versiones de software, direccionamiento IP, software que usa, tipos y versión de las herramientas de seguridad que protegen, etc. - - - (…) - - - Considerando lo anterior, cabe reiterar que la información solicitada por el ciudadano debe ser considerada como restringida, toda vez que su divulgación puede proporcionar información sensible de la operación y seguridad de los servicios publicados en Internet de la SCJN, derivando en ataques informáticos, afectación y degradación de los servicios de información.*

Escenario	*Implicación*	*Daño o afectación*
Dar a conocer los tipos de ataques recibidos a los portales web de la SCJN	*Cada una de las herramientas de seguridad informática tiene una clasificación propia para la identificación de cada uno de los tipos de ataques informáticos. Esto implica dar a conocer la marca de equipos de seguridad informática que hace uso la SCJN.* *Reconocimiento del tipo de ataques web que se han recibido y mitigado en los portales web.*	• *Aumento de ataques informáticos específicos contra las versiones y marca de los equipos de seguridad informática identificados.* • *Capacidad para identificar la versión de firmware del equipo de seguridad, con lo cual podrían explotar una vulnerabilidad y modificar sin autorización los portales web de la SCJN.*

Escenario	*Implicación*	*Daño o afectación*
		• *Recepción de ataques no recibidos o identificados en la infraestructura de seguridad informática, llegando a afectar el contenido de los portales web.*
Dar a conocer la cantidad y periodo de ataques informáticos.	*Implicaría conocer la cantidad de peticiones web que puede soportar la infraestructura tecnológica de comunicaciones, seguridad y de servidores de la SCJN para sus portales web.*	• *Aumento de ataques informáticos dirigidos a superar la volumetría del canal de comunicación de los portales de Internet, toda vez que el ancho de banda tiene un límite de consumo, evitando con ello el acceso a los portales por parte de usuarios y servidores públicos.* • *Superar la capacidad de operación de los equipos servidores, de comunicaciones o de seguridad informática, lo que causaría la caída total del servicio.*
Dar a conocer el lugar de origen de los ataques web.	*Implica reconocer los lugares donde no se cuenta con un filtrado de peticiones, es decir que pueden llegar hasta la infraestructura de los portales web de la SCJN.*	• *Aumento de ataques informáticos desde regiones o zonas donde se tiene permitido el flujo de tráfico hacia los portales de Internet de la SCJN, lo que agotaría el enlace de comunicación de los portales web de la*

CONCLUSIONES: *El proporcionar la información solicitada, facilita a potenciales atacantes llamados "watering hole", conocer el nivel de vulnerabilidades de conexiones que existen en los sitios, el dar el número de ataques, permite a través de la estadística, identificar el estado que guarda nuestra infraestructura, lo cual no es recomendable, ni de uso cotidiano para la ciudadanía, solo expertos en la materia requieren información tan especializada." [sic]*

Por último, se precisa que no se ha procedido a levantar alguna denuncia penal, a través de la instancia competente, toda vez que solo han sido intentos de ataques cibernéticos."

V. Vista a la Secretaría del Comité de Transparencia. Mediante correo electrónico de veintiuno de enero de dos mil veintiuno, el Titular de la Unidad General de Transparencia y Sistematización de la Información Judicial remitió el oficio UGTSIJ/TAIPDP/0219/2021 y el

expediente electrónico UT-A/0002/2021 a la Secretaría del Comité de Transparencia, con la finalidad de que se dictara la resolución correspondiente.

VI. Acuerdo de turno. Mediante acuerdo de veintiuno de enero de dos mil veintiuno, la Presidencia del Comité de Transparencia, con fundamento en los artículos 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública, así como 23, fracción II, y 27, del Acuerdo General de Administración 5/2015, ordenó integrar el expediente **CT-CI/A-2-2021** y, conforme al turno correspondiente, remitirlo al Contralor del Alto Tribunal, a fin de que presentara la propuesta de resolución, lo que se hizo mediante oficio CT-27-2021, enviado mediante correo electrónico en la misma fecha.

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

PRIMERO. 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 II y III, de la Ley General de Transparencia y Acceso a la Información Pública, 65, fracciones II y III, de la Ley Federal de Transparencia y Acceso a la Información Pública, así como 23, fracciones II y III, del Acuerdo General de Administración 5/2015.

SEGUNDO. Análisis. En la solicitud se pide información de la Suprema Corte de Justicia de la Nación, consistente en:

1. Número de ataques cibernéticos de enero de 2020 al 4 de enero de 2021, en que se recibió la solicitud.
2. Detalle de los ataques por tipo, país de procedencia y tipo de afectación.
3. Informe sobre si se levantó denuncia penal y, en su caso, si hubo detenido.

I. Información que se pone a disposición.

Por cuanto a la información que se solicita en el punto 1, relativa a la cantidad de ataques cibernéticos, en la nota del Director de Seguridad Informática y del Jefe de Departamento de Criptografía y Autentificación de la Dirección General de Tecnologías de la Información se informa que de enero de 2020 al 7 de enero de 2021, la Suprema Corte de Justicia de la Nación recibió 1,234 (mil doscientos treinta y cuatro) intentos de ataques cibernéticos, desglosando en una tabla el número de éstos de manera mensual, por lo que con esa información se tiene por atendido lo requerido en ese aspecto.

Cabe señalar que, si bien en el informe que fue materia de análisis en el cumplimiento CT-CUM/A-36-2018, la Dirección General de Tecnologías de la Información propuso la reserva del número de ataques, el Comité de Transparencia validó la publicidad de esa información.

De igual forma, se tiene por atendido lo planteado en el punto 3, pues en la referida nota se precisa que no se levantó denuncia penal alguna, puesto que sólo se trató de intentos de ataques cibernéticos, de lo que se sigue que no se tiene información de algún detenido por esos

hechos, ni de afectaciones a este Alto Tribunal, atendiendo con esto último lo requerido en el punto 2 sobre el tipo de afectación.

De conformidad con lo expuesto, se solicita a la Unidad General de Transparencia que haga llegar al peticionario la información proporcionada por la Dirección General de Tecnologías de la Información en la nota a que se ha hecho referencia, dado que con ello se atiende lo planteado en los puntos 1, 2, respecto del tipo de afectación y 3.

II. Información reservada.

Por cuanto a lo requerido sobre el tipo de ataque y país de procedencia mencionados en el punto 2, en la nota del Director de Seguridad Informática y del Jefe de Departamento de Criptografía y Autentificación se clasifica dicha información como reservada, haciendo referencia a la resolución CT-CUM/A-36-2018.

Para llevar a cabo el análisis correspondiente, se tiene en cuenta que en el esquema de nuestro sistema constitucional, el derecho de acceso a la información encuentra cimiento en lo dispuesto en el artículo 6º, apartado A, de la Constitución Política de los Estados Unidos Mexicanos, cuyo contenido deja claro que, en principio, todo acto de autoridad (todo acto de gobierno) es de interés general y, por ende, es susceptible de ser conocido por todos.

Sin embargo, como lo ha interpretado el Pleno del Alto Tribunal en diversas ocasiones, el derecho de acceso a la información no puede caracterizarse como uno de contenido absoluto, en tanto su ejercicio se

encuentra acotado en función de ciertas causas e intereses relevantes, así como frente al necesario tránsito de las vías adecuadas para ello[1].

En atención al dispositivo constitucional antes referido, la información que tienen bajo su resguardo los sujetos obligados del Estado encuentra como excepción aquella que sea temporalmente reservada o confidencial en los términos establecidos por el legislador federal o local, cuando de su propagación pueda derivarse perjuicio por causa de interés público y seguridad nacional.

Para sustentar la clasificación de reserva que hace la Dirección General de Tecnologías de la Información, transcribe el informe que fue materia de análisis en el cumplimiento CT-CUM/A-36-2018, en el que se manifestó, substancialmente, lo siguiente:

- Proporcionar el tipo de ataques permitiría aumentar los ataques informáticos de manera específica contra las versiones y marca de los equipos de seguridad, así como recepción de otros ataques no recibidos o identificados previamente.

[1] ***DERECHO A LA INFORMACIÓN. SU EJERCICIO SE ENCUENTRA LIMITADO TANTO POR LOS INTERESES NACIONALES Y DE LA SOCIEDAD, COMO POR LOS DERECHOS DE TERCEROS****. El derecho a la información consagrado en la última parte del artículo 6o. de la Constitución Federal no es absoluto, sino que, como toda garantía, se halla sujeto a limitaciones o excepciones que se sustentan, fundamentalmente, en la protección de la seguridad nacional y en el respeto tanto a los intereses de la sociedad como a los derechos de los gobernados, limitaciones que, incluso, han dado origen a la figura jurídica del secreto de información que se conoce en la doctrina como "reserva de información" o "secreto burocrático". En estas condiciones, al encontrarse obligado el Estado, como sujeto pasivo de la citada garantía, a velar por dichos intereses, con apego a las normas constitucionales y legales, el mencionado derecho no puede ser garantizado indiscriminadamente, sino que el respeto a su ejercicio encuentra excepciones que lo regulan y a su vez lo garantizan, en atención a la materia a que se refiera; así, en cuanto a la seguridad nacional, se tienen normas que, por un lado, restringen el acceso a la información en esta materia, en razón de que su conocimiento público puede generar daños a los intereses nacionales y, por el otro, sancionan la inobservancia de esa reserva; por lo que hace al interés social, se cuenta con normas que tienden a proteger la averiguación de los delitos, la salud y la moral públicas, mientras que por lo que respecta a la protección de la persona existen normas que protegen el derecho a la vida o a la privacidad de los gobernados. Época: Novena Época. Registro: 191967. Instancia: Pleno. Tipo de Tesis: Aislada. Fuente: Semanario Judicial de la Federación y su Gaceta. Tomo XI, Abril de 2000. Materia(s): Constitucional Tesis: P. LX/2000. Página: 74)*

- Proporcionar el lugar (lugar de procedencia) permitiría que se aumente el número de ataques desde regiones o zonas donde se tiene permitido el flujo de tráfico hacia los portales de internet de este Alto Tribunal.

Los argumentos expuestos en la resolución CT-CUM/A-36-2018, permiten confirmar que la información requerida se clasifica como **reservada**, con apoyo en el artículo 113, fracción I, de la Ley General de Transparencia, en virtud de que se podrían poner en riesgo cuestiones de seguridad pública, pues si se divulgara la información solicitada, posibilitaría el aumento de los ataques informáticos, de manera específica contra las versiones y marca de los equipos de seguridad desde regiones o zonas donde se tiene permitido el flujo de tráfico hacia los portales de internet de este Alto Tribunal.

En ese tenor, debe destacarse que el informe lo emite el área técnica que, conforme a sus atribuciones, es responsable del manejo de los equipos a través de los cuales se gestiona la información, por lo que considerando lo resuelto por este Comité en el expediente CT-CUM/A-36-2018, se arriba a la conclusión que sobre la información requerida sí pesa la reserva establecida en la fracción I, del artículo 113, de la Ley General de Transparencia 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;"*
> (…)

En efecto, acorde con lo resuelto por este Comité en la resolución CT-CUM/A-36-2018, *"desde una óptica general, el objeto de la*

restricción de la información, como se ha visto, comprende garantizar el buen funcionamiento de los sistemas de seguridad informáticos ante posibles ataques cibernéticos[2], que en general pondrían en riesgo la información de este Alto Tribunal (tanto del quehacer jurisdiccional como administrativo), y con ello daría lugar su posible extracción, modificación o alteración, lo que en última instancia comprometería el ejercicio de los derechos de las personas (acceso a la justicia), lo que es concordante con lo establecido en el artículo décimo octavo, párrafo primero, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de las versiones públicas emitidos por el Sistema Nacional de Transparencia[3]".

Aunado a lo anterior, se precisó que *"que resulta imperante que se cuenten con sistemas de seguridad basados, entre otros elementos, en una gestión que considere la prevención, detección y respuesta inmediata a los incidentes que afecten a los sistemas en general, tal y como lo disponen los principios 7 y 8 de las Directrices para la seguridad de sistemas y redes de información: hacia una cultura de seguridad[4]*

---

[2] 'Según el Instituto Nacional de Estándares y Tecnologías (NIST, por sus siglas en inglés), ataque cibernético o "ciberataque", podría comprender "un intento de obtener acceso no autorizado a servicios, recursos o información, o un intento de comprometer la integridad, disponibilidad o confidencialidad del sistema" (visible en la siguiente página: https://csrc.nist.gov/Glossary/?term=3015#AlphaIndexDiv). Inclusive se encuentra tipificado como delito por el artículo 211 bis 2, del Código Penal Federal.'

[3] 'Décimo octavo. De conformidad con el artículo 113, fracción I de la Ley General, podrá considerarse como información reservada, aquella que comprometa la seguridad pública, al poner en peligro las funciones a cargo de la Federación, la Ciudad de México, los Estados y los Municipios, tendientes a preservar y resguardar la vida, la salud, la integridad y el ejercicio de los derechos de las personas, así como para el mantenimiento del orden público…"

*[4] '**7) Diseño y realización de la seguridad. Los participantes deben incorporar la seguridad como un elemento esencial de los sistemas y redes de información.***
Los sistemas, las redes y las políticas deberán ser diseñados, ejecutados y coordinados de manera apropiada para optimizar la seguridad. Un enfoque mayor pero no exclusivo de este esfuerzo ha de encontrarse en el diseño y adopción de mecanismos y soluciones que salvaguarden o limiten el daño potencial de amenazas o vulnerabilidades identificadas. Tanto las salvaguardas técnicas como las no técnicas así como las soluciones a adoptar se hacen imprescindibles, debiendo ser proporcionales al valor de la información de los sistemas y redes de información. La seguridad ha de ser un elemento fundamental de todos los productos, servicios, sistemas y redes; y una parte integral del diseño y arquitectura de los sistemas. Para los usuarios finales el diseño e implementación de la seguridad radica fundamentalmente en la selección y configuración de los productos y servicios de sus sistemas.

(directrices), de la OCDE (por sus siglas en inglés: Organisation for Economic Cooperation and Development)”.

En ese sentido, se tiene presente que en términos del artículo 100, último párrafo, de la Ley General de Transparencia[5], en relación con el 17, párrafo primero, del Acuerdo General de Administración 5/2015[6], es competencia del titular de la instancia que tiene bajo resguardo la información requerida, determinar su disponibilidad y clasificarla conforme a los criterios establecidos en la normativa aplicable.

Así, conforme a lo anterior, la Dirección General de Tecnologías de la Información es el área técnica que cuenta con el personal especializado para velar por la seguridad de la información y de los sistemas tecnológicos del Alto Tribunal, en términos de lo establecido en el artículo 27, fracción I, del Reglamento Orgánico en Materia Administrativa de la Suprema Corte de Justicia de la Nación[7].

---

8) Gestión de la Seguridad.
Los participantes deben adoptar una visión integral de la administración de la seguridad. La gestión de la seguridad debe estar basada en la evaluación del riesgo y ser dinámica, debiendo comprender todos los niveles de las actividades de los participantes y todos los aspectos de sus operaciones. Asimismo ha de incluir posibles respuestas anticipadas a riesgos emergentes y considerar la prevención, detección y respuesta a incidentes que afecten a la seguridad, recuperación de sistemas, mantenimiento permanente, revisión y auditoría. Las políticas de seguridad de los sistemas y redes de información, así como las prácticas, medidas y procedimientos deben estar coordinadas e integradas para crear un sistema coherente de seguridad. Las exigencias en materia de gestión de seguridad dependerán de los niveles de participación, del papel que desempeñan los participantes, del riesgo de que se trate y de los requerimientos del sistema…’

[5] ***“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.”

[6] ***“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…”

[7] *“**Artículo 27.** El Director General de Tecnologías de la Información tendrá las siguientes atribuciones:*
I. Administrar los recursos en materia de tecnologías de la información y comunicación y proveer los servicios que se requieran en la materia;”
(…)

En ese sentido, tratándose de cuestiones que atañen a la protección específica de los rubros que involucran aspectos vinculados con la seguridad de los sistemas tecnológicos del Alto Tribunal, es claro que cuando el área enteramente responsable ubica el surgimiento de elementos que inciden en la dimensión ya señalada, el órgano encargado de conocer del acceso sólo debe limitarse a entender y valorar la razonabilidad de la clasificación expresada para efecto de su confirmación o no.

De manera similar a lo argumentado en la resolución CT-CUM/A-36-2018, este Comité de Transparencia identifica que se pretende proteger, desde un esquema global, la infraestructura de seguridad informática de este Alto Tribunal, en tanto que se podrían involucrar negativamente aspectos de seguridad pública, y con ello facilitar un ataque cibernético, con repercusiones como son, por una parte, facilitar la extracción, modificación o alteración de información sensible de los expedientes jurisdiccionales, lo que incide directamente en su tarea sustantiva y, por otra parte, *"comprometerse la información administrativa, que generaría un probable riesgo a las personas en lo particular como son trabajadores y proveedores, al hacerse patente un acceso no autorizado ni controlado a los datos personales que se tengan registrados, inclusive, a información contable o bancaria, por solo citar algunos casos."*

De conformidad con los argumentos señalados, este Comité de Transparencia **confirma la clasificación reservada** de la información relativa al tipo de ataque cibernético y lugar de origen (país de

procedencia), con fundamento en el artículo 113, fracción I, de la Ley General de Transparencia.

Con base en lo hasta aquí dicho, este Comité estima que la clasificación antes advertida también se sustenta, desde la especificidad que en aplicación de la prueba de daño mandatan los artículos 103 y 104 de la Ley General, cuya delimitación, como se verá enseguida, necesariamente debe responder a la propia dimensión del supuesto de reserva con el que se relacione su valoración.

Lo anterior, porque se podrían poner en riesgo cuestiones de seguridad pública, pues según se señaló previamente, a partir de los datos solicitados, si se divulgaran, sería posible perfeccionar un ataque cibernético, o bien intentos de otros no recibidos o identificados hasta el momento, al contar con factores de reconocimiento sobre la infraestructura de seguridad informática de la Suprema Corte de Justicia de la Nación, a partir de los ataques registrados y mitigados, lo que evidentemente si pesa sobre la capacidad de respuesta.

En ese orden de ideas, lo que se impone es **clasificar** como reservada la información a que se hace referencia en este apartado, 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[8] de la Ley General de Transparencia.

---

[8] ***"Artículo 101.*** *Los Documentos clasificados como reservados serán públicos cuando:*
I. Se extingan las causas que dieron origen a su clasificación;
II. Expire el plazo de clasificación;
III. Exista resolución de una autoridad competente que determine que existe una causa de interés público que prevalece sobre la reserva de la información, o
IV. El Comité de Transparencia considere pertinente la desclasificación, de conformidad con lo señalado en el presente Título.

Por lo expuesto y fundado; se,

R E S U E L V E:

PRIMERO. Se tiene por atendida la solicitud respecto de lo expuesto en el considerando segundo, apartado I, de la presente resolución.

SEGUNDO. Se confirma la clasificación de reservada, de la información a que se hace referencia en el apartado II del segundo considerando de esta resolución.

TERCERO. Se requiere a la Unidad General de Transparencia para que realice las acciones señaladas en esta resolución.

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

Por unanimidad de votos lo resolvió el Comité de Transparencia de la Suprema Corte de Justicia de la Nación, integrado por el maestro Luis Fernando Corona Horta, Director General de Asuntos Jurídicos y

---

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.
Excepcionalmente, los sujetos obligados, con la aprobación de su Comité de Transparencia, podrán ampliar el periodo de reserva hasta por un plazo de cinco años adicionales, siempre y cuando justifiquen que subsisten las causas que dieron origen a su clasificación, mediante la aplicación de una prueba de daño.
Para los casos previstos por la fracción II, cuando se trate de información cuya publicación pueda ocasionar la destrucción o inhabilitación de la infraestructura de carácter estratégico para la provisión de bienes o servicios públicos, o bien se refiera a las circunstancias expuestas en la fracción IV del artículo 113 de esta Ley y que a juicio de un sujeto obligado sea necesario ampliar nuevamente el periodo de reserva de la información; el Comité de Transparencia respectivo deberá hacer la solicitud correspondiente al organismo garante competente, debidamente fundada y motivada, aplicando la prueba de daño y señalando el plazo de reserva, por lo menos con tres meses de anticipación al vencimiento del periodo."

Presidente del Comité, Maestro Christian Heberto Cymet López Suárez, Contralor del Alto Tribunal, y Maestro Julio César Ramírez Carreón, Titular de la Unidad General de Investigación de Responsabilidades Administrativas; quienes firman con el secretario del Comité que autoriza.

MAESTRO LUIS FERNANDO CORONA HORTA
PRESIDENTE DEL COMITÉ

MAESTRO CHRISTIAN HEBERTO CYMET LÓPEZ SUÁREZ
INTEGRANTE DEL COMITÉ

MAESTRO JULIO CÉSAR RAMÍREZ CARREÓN
INTEGRANTE DEL COMITÉ

LICENCIADO ARIEL EFRÉN ORTEGA VÁZQUEZ
SECRETARIO 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."