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

CUMPLIMIENTO CT-CUM/A-52-2023
derivado del expediente CT-CUM/A-36/2018

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 **ocho de noviembre de dos mil veintitrés**.

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

I. Solicitud de información. El cinco de julio de dos mil dieciocho se recibió en la Plataforma Nacional de Transparencia la solicitud tramitada bajo el folio 0330000135418, requiriendo:

> *"…conocer el número de ataques cibernéticos que la dependencia federal ha recibido de enero de 2018 a la fecha. Favor de detallar por mes, tipo de ataque y lugar de origen".* [sic]

II. Resolución del Comité de Transparencia. En sesión de cinco de septiembre de dos mil dieciocho este Comité de Transparencia emitió resolución en el expediente **CT-CI/A-20-2018**[1], en la parte que interesa, en los términos siguientes:

> *"[…]*
> ***II. Análisis.*** *Como se vio en el capítulo de antecedentes, la petición que propició la integración del presente asunto se centra en diversa información sobre posibles ataques cibernéticos que este Alto Tribunal hubiere recibido a partir de enero de este año a la fecha.*
>
> *Al enfrentarse a tal solicitud; el Director General de Tecnologías de la Información entendió que la divulgación de esa información podría comprometer, en distintos aspectos, la infraestructura tecnológica de este Alto Tribunal; de ahí que procedió a su reserva en términos del artículo 113 fracción XI, de la Ley General.*
>
> *Sobre esa base, el punto a dilucidar a través del caso que nos ocupa radica en determinar si sobre la información requerida se actualiza o no la reserva identificada por el área instada a su divulgación y, en su caso, si aquella puede o no ser proporcionada en los términos solicitados.*

[1] Disponible en: CT-CI-A-20-2018.pdf (scjn.gob.mx)

x1/iAQw9lPZGQkEmApJv5g8vd+u8zWPKvjVyNm1uO8s=

Ahora, antes de llevar a cabo el análisis correspondiente, es importante recordar que en el esquema de nuestro sistema constitucional, el derecho de acceso a la información encuentra cimiento a partir de lo dispuesto en el artículo 6º, apartado A, de la Constitución, 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[2]*.*

Así, precisamente en atención al dispositivo constitucional antes referido, se obtiene que 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.

Trasladado al caso, como se vio en el apartado de antecedentes, para sustentar la reserva debatida, el área manifestó expresamente que divulgar lo solicitado pondría en riesgo la información de la institución porque:

- *Revelar la cantidad de peticiones web podría evidenciar la capacidad de la infraestructura tecnológica y de seguridad, y en su caso, la posibilidad de recibir mayores ataques, con la consecuente caída de los portales de Internet de la Institución;*
- *Identificar el tipo de ataques detectados, permitiría dirigir éstos de manera específica por vía de eliminación;*
- *Dar a conocer el lugar de los ataques podría generar otros coordinados desde distintos lugares.*

*En ese sentido, la instancia entendió que la información se encontraba **reservada**, al estimar actualizada la hipótesis dispuesta en el artículo 113, fracción*

---

[2] ***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)

x1/iAQw9lPZGQkEmApJv5g8vd+u8zWPKvjVyNm1uO8s=

XI, de la Ley General, en virtud de que se podrían poner en riesgo cuestiones de seguridad informática y, con ello, de la conducción de expedientes judiciales o procedimientos administrativos seguidos en forma de juicio.

El referido dispositivo establece:

*'**Artículo 113**. Como información reservada podrá clasificarse aquella cuya publicación:*
…;
XI. Vulnere la conducción de los Expedientes judiciales o de los procedimientos administrativos seguidos en forma de juicio, en tanto no hayan causado estado;..'

Al respecto, el contraste entre la justificación proporcionada por el área requerida y los supuestos contenidos en el precepto transcrito, permiten evidenciar que dicha motivación resulta indebida, ya que si bien es cierto que, en principio, como este Comité ha sostenido en otros asuntos[3], la posible afectación de los sistemas tecnológicos de este Alto Tribunal podría generar un acceso no controlado y no permitido a la información de los expedientes judiciales o procedimientos administrativos seguidos en forma de juicio, también lo es que junto a la tarea sustantiva de este Tribunal Constitucional, que se traduce en la emisión de sentencias dentro de los diversos expedientes de los que toca conocer, prevalecen múltiples actividades administrativas para su debido desarrollo, sobre cuya vigencia, en este caso, no podría entenderse actualizada la hipótesis ya descrita.

En efecto, como se dijo al resolver la clasificación de información CT-CI/A-3-2018, en sesión de dieciocho de abril del presente año, 'no todo el cúmulo de herramientas o instrumentos tecnológicos con los que opera la Suprema Corte de Justicia de la Nación se encuentran vinculados o referenciados con los expedientes judiciales, sino que también prevalecen sistemas orientados a la gestión de su administración (recursos humanos, adquisiciones, contabilidad, etcétera)', de ahí que, por tal motivo, en estos casos la materialización de la causa de reserva no puede predicarse de manera general o abstracta, siendo que, además, tal supuesto se limita al espacio de los expedientes judiciales.

En otro orden de ideas, esas consideraciones dan cuenta que, para efectos del acceso a la información, la supuesta alteración del esquema de seguridad de los sistemas tecnológicos sobre los que puede descansar la dinámica de comunicación y operación de los diversos sujetos obligados debe justificarse de manera concreta y estricta, sin que la mera posibilidad de ataques sea suficiente para ello.

Sobre todo porque el acceso a la información no puede entenderse sustentado en un principio de riesgo futuro o de malicia de quien acude a su ejercicio, de ahí que su eficacia no deba verse obstaculizada a partir de supuestas categorías y datos técnicos generales e hipotéticos, sino que, por el contrario, para su posible limitación se exige la precisión de datos objetivos que, dentro de un marco racional específico, demuestren de modo <u>real</u> y excepcional el daño que la divulgación de la información representaría, en términos de los artículos 104 y 113 de la Ley General, lo que no aconteció en la especie, sin que este Comité, en este momento, pueda pronunciarse al respecto.

x1/iAQw9lPZGQkEmApJv5g8vd+u8zWPKvjVyNm1uO8s=

[3] *Tal como fue el CT-CI/A-7-2018, de treinta de mayo de este año.*

Ello, de conformidad con lo dispuesto en los artículos 100, último párrafo de la Ley General[4], en relación con el 17, párrafo primero, de los Lineamientos Temporales[5], en tanto es competencia del titular de la instancia que tiene bajo su resguardo la información requerida, determinar su disponibilidad y clasificarla conforme a los criterios establecidos en la normativa aplicable, además de que es la única 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 dispuesto por el artículo 27, fracción XI del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación[6].

Luego, conforme a lo anterior, ante la evidencia de la necesidad de proteger información que pudiere generar afectación a los sistemas de seguridad informática, que pudieren incidir en accesos no controlados ni permitidos de la información, tanto jurisdiccional como administrativa, de este Alto Tribunal, se exigiría que se precise y justifique de forma suficiente, desde la especifica prueba de daño, la reserva de información a que se ha venido haciendo mención o alguna otra.

Junto a lo anterior, y solo a manera de ejemplo, se tiene que algunos sujetos obligados, como es el caso del Banco de México y el Centro de Investigación y Seguridad Nacional 'Cisen'[7], han informado, en mayor o menor medida, sobre los ciberataques de los que han sido objeto, lo que refuerza la idea de que se explique con mayor precisión, para cada punto planteado en la solicitud de acceso, porqué podría determinarse la reserva, o bien, porqué sería factible la divulgación.

Por tanto, de conformidad con lo dispuesto por el artículo 37, párrafos primero y segundo, de los Lineamientos Temporales[8], se ***requiere*** *al Director General de Tecnologías de la Información, para que, en el plazo de cinco días hábiles, computados a partir del día siguiente al en que surta sus efectos la notificación de la presente resolución, justifique, desde la especifica prueba de*

---

[4] '***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.'

[5] '***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…'

[6] '***Artículo 27.*** *El Director General de Tecnologías de la Información tendrá las siguientes atribuciones:*
…
XI. Ejecutar y actualizar los mecanismos de seguridad informática y vigilar su adecuado funcionamiento;…'

[7] *En este caso, se puede consultar la resolución del recurso de revisión 155/11 resuelto por el entonces Instituto Federal de Acceso a la Información y Protección de Datos Personales, en la cual se observa que el CISEN, en la etapa de alegatos, informó a ese Instituto el número de ataques informáticos detectados por el órgano desconcentrado en su contra en el periodo de dos mil nueve a dos mil diez; dando por resultado, en lo que importa, que se instruyera al sujeto obligado a comunicar al peticionario el dato referido.*
Dicha resolución está visible en la siguiente liga:
file:///D:/Users/lfuentesm/Downloads/155%20(1).pdf

[8] '***Artículo 37***
Del cumplimiento de las resoluciones
Las resoluciones del Comité que ordenen acciones concretas a las instancias, deberán cumplirse dentro del plazo de cinco días hábiles a partir de su notificación.
Además del cumplimiento, las instancias deberán informar al Secretario y, en su caso, remitirle las constancias que lo acrediten dentro del plazo establecido en el párrafo anterior...'

x1/iAQw9lPZGQkEmApJv5g8vd+u8zWPKvjVyNm1uO8s=

daño, la reserva de información, de acuerdo a la causal o hipótesis respectiva de las encausadas en el artículo 113 de la Ley General.

Por lo expuesto y fundado; se,

R E S U E L V E:

***ÚNICO**. Se requiere al Director General de Tecnologías de la Información, en términos de lo expuesto en esta resolución.*
[…].”

III. Resolución de Cumplimiento. En sesión de trece de noviembre de dos mil dieciocho este Comité de Transparencia resolvió el expediente CT-CUM/A-36/2018[9], en el cual, en la parte de interés, se determinó lo siguiente:

“[…]
***II. Cumplimiento de la resolución del Comité de Transparencia.** Corresponde analizar si se dio cumplimiento a la resolución de fecha cinco de septiembre de dos mil dieciocho, emitida dentro de la clasificación de información CT-CI/A-20-2018.*

Ahora, se recuerda que en la resolución de mérito, este órgano colegiado identificó que no podía entenderse actualizada la causal de reserva que establece la fracción XI, de la Ley General, no obstante, también se dijo que ante la evidencia de la necesidad de proteger información que pudiere generar afectación a los sistemas de seguridad informática, se exigía precisión, desde la prueba de daño, a efecto de estar en la posibilidad de reservar la información solicitada.

Ello porque, como también se dijo al resolver la clasificación de información CT-CI/A-20-2018, 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[10].

x1/iAQw9lPZGQkEmApJv5g8vd+u8zWPKvjVyNm1uO8s=

[9] Disponible en: Microsoft Word - CumA 36 2018 F (scjn.gob.mx)

[10] ***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)

De lo cual se obtiene que 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 o pública.

Conforme a esto, el Director General de Tecnologías de la Información, sin precisar causal de reserva alguna, a grandes rasgos dijo que la divulgación de los datos solicitados podría exponer la capacidad de reacción de los sistemas de seguridad informáticos y propiciar el aumento y especificidad de ataques cibernéticos, al proporcionar información sensible de la operación y seguridad de los servicios publicados en Internet de este Alto Tribunal, ya que implicaría lo siguiente:

- *De la cantidad y periodo de peticiones o ataques soportados, ante el límite de consumo de banda, podría generar que se reciba una cantidad superior al volumen del canal de comunicación, y con ello se causaría la caída de los portales de Internet de la Institución;*
- *Sobre 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;*
- *Del lugar, 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.*

Con lo anterior, se tiene que se ha dado cumplimiento a lo ordenado por este órgano colegiado, por parte de la instancia requerida, correspondiendo ahora realizar el estudio concreto de la clasificación de información.

Así, dada la motivación que da el área, se arriba a la conclusión que, en su caso y como se verá, pesaría la reserva establecida en la fracción I, del artículo 113, de la Ley General, que establece lo siguiente:

> *'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;…'*

Esto porque, 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[11], 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

---

[11] 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.

x1/iAQw9lPZGQkEmApJv5g8vd+u8zWPKvjVyNm1uO8s=

información, así como para la elaboración de las versiones públicas emitidos por el Sistema Nacional de Transparencia[12]*.*

Aunado a 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[13] *(directrices), de la OCDE (por sus siglas en inglés: Organisation for Economic Coooperation and Development).*

Por otra parte, una vez identificada la causal de reserva, debe tenerse en cuenta que de conformidad con lo dispuesto en los artículos 100, último párrafo de la Ley General[14]*, en relación con el 17, párrafo primero, de los Lineamientos Temporales*[15]*, es competencia del titular de la instancia que tiene bajo su resguardo la información requerida, determinar su disponibilidad y clasificarla conforme a los criterios establecidos en la normativa aplicable.*

Conforme a lo anterior, se tiene que la Dirección General de Tecnologías de la Información es la área técnica [sic] *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 por el artículo 27, fracción I, del*

---

[12] ‘***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…’*

[13] ‘***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.
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…’

[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.’

[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…’

x1/iAQw9lPZGQkEmApJv5g8vd+u8zWPKvjVyNm1uO8s=

Reglamento Orgánico en Materia Administrativa de la Suprema Corte de Justicia de la Nación[16]*.*

En ese sentido, tratándose de cuestiones que atañen a la protección específica de los rubros que involucran aspectos vinculados con la infraestructura se seguridad informática 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/o valorar la razonabilidad de la clasificación expresada para efecto de su confirmación o no.

Precisado lo anterior, corresponde ahora analizar, desde la razonabilidad de la motivación expresada por el área, si los datos específicamente requeridos (número, tipo y lugar de origen de los ataques cibernéticos que se hubieren presentado en esta Suprema Corte de Justicia de la Nación) darían lugar o no a la clasificación total de la información solicitada.

a) Tipo y lugar de origen de los ataques cibernéticos. *Por cuanto estos datos, ante la razón desprendida de los informes presentados por el área requerida y responsable, este Comité de Transparencia identifica, como se ha venido señalando, 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, e inclusive información contable o bancaria, por solo citar algunos casos.*

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 relaciona su valoración.

Lo anterior, porque, se podrían poner en riesgo cuestiones de seguridad pública, pues según se refirió previamente, a partir de la información solicitada, si se divulgara, 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, como se anunciaba previamente, lo que se impone es ***confirmar*** *la determinación del área, para efecto de confirmar la reserva de la información solicitada, por un plazo de cinco años en atención a lo establecido por el artículo 101*[17]*, de la Ley General.*

---

[16] ‘***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;…’

[17] ‘***Artículo 101.*** *Los Documentos clasificados como reservados serán públicos cuando:*

x1/iAQw9lPZGQkEmApJv5g8vd+u8zWPKvjVyNm1uO8s=

b) Número de ataques cibernéticos. *Sobre este apartado, se tiene que el área responsable dijo que dar a conocer la cantidad y periodo de ataques informáticos podría generar un aumento dirigido a superar la volumetría del canal de comunicación.*

Sin embargo, se considera que es factible dar a conocer, de forma global, el número de ataques cibernéticos que ha recibido este Alto Tribunal del uno de enero al cinco de julio de este año.

Lo anterior en virtud de que, por una parte, si bien es cierto que la volumetría posiblemente influiría en la cantidad de ataques cibernéticos, ello no trascendería en la forma o base de éstos, que podría repercutir en su perfeccionamiento, aunado a que la determinación del número de intentos puede erigirse por la simple voluntad de los actores.

Por otra parte, y sobre todo, debe tomarse en cuenta que, conforme a los principios 1, 3 y 5, de las directrices[18], la seguridad de los sistemas y redes de

---

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.

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.'

*[18] '**1) Concienciación***
Los participantes deberán ser conscientes de la necesidad de contar con sistemas y redes de información seguros, y tener conocimiento de los medios para ampliar la seguridad.
El conocimiento de los riesgos y de los mecanismos disponibles de salvaguardia, es el primer paso en la defensa de la seguridad de los sistemas y redes de información. Estos sistemas y redes de información pueden verse afectados tanto por riesgos internos como externos. Los participantes deben comprender que los fallos en la seguridad pueden dañar significativamente los sistemas y redes que están bajo su control. Deben asimismo ser conscientes del daño potencial que esto puede provocar a otros derivados de la interconexión y la interdependencia. Los participantes deben tener conocimiento de las configuraciones y actualizaciones disponibles para sus sistemas, así como su lugar que ocupan dentro de las redes, las prácticas a ejecutar para ampliar la seguridad, y las necesidades del resto de los participantes.
3) Respuesta
Los participantes deben actuar de manera adecuada y conjunta para prevenir, detectar y responder a incidentes que afecten la seguridad.
Al reconocer la interconexión de los sistemas y de las redes de información, así como el riesgo potencial de un daño que se extienda con rapidez y tenga una [sic] alcance amplio, los participantes deben actuar de manera adecuada y conjunta para enfrentarse a los incidentes que afecten la seguridad. Asimismo han de compartir información sobre los riesgos y vulnerabilidades y ejecutar procedimientos para una cooperación rápida y efectiva que permita prevenir, detectar y responder a

x1/iAQw9lPZGQkEmApJv5g8vd+u8zWPKvjVyNm1uO8s=

información habrán de ser consistentes con los valores de concienciación, respuesta y democracia, es decir, partir del conocimiento de los riesgos potenciales para actuar de forma adecuada, lográndose de manera consistente con la garantía de derechos reconocidos como son la protección de la información personal, la apertura y la transparencia.

Así, el factor de conocimiento del número de ataques si es viable de entrega, dado que es relevante que la sociedad y las personas que en concreto se relacionan con este Alto Tribunal (por ser trabajadores, proveedores o usuarios del sistema judicial, por citar algunos casos) tengan un parámetro de entendimiento y confianza sobre la seguridad de resguardo de sus datos, conforme a la capacidad de afrontar los riesgos de ciberataques, de ahí que, como se dijo en la clasificación de información CT-CI/A-20-2018: 'el acceso a la información no puede entenderse sustentado en un principio de riesgo futuro o de malicia de quien acude a su ejercicio'.

*En consecuencia, se **revoca** la clasificación efectuada por el área con relación al número de ataques cibernéticos que ha recibido este Alto Tribunal del uno de enero al cinco de julio de este año.*

*Por tanto, de conformidad con lo dispuesto por el artículo 37, párrafo quinto, de los Lineamientos Temporales[19], se **requiere** al Director General de Tecnologías de la Información, para que en el plazo de dos días hábiles, computados a partir del día siguiente al en que surta sus efectos la notificación de la presente resolución, remita a la Unidad General de Transparencia y Sistematización de la Información Judicial, el informe de forma global, sobre el número de ataques cibernéticos que ha recibido este Alto Tribunal del uno de enero al cinco de julio de este año, para ésta a su vez comunique el dato a la persona solicitante.*

Por lo expuesto y fundado; se,

R E S U E L V E:

***PRIMERO**. Se tiene por atendido el requerimiento efectuado a la Dirección General de Tecnologías de la Información.*

***SEGUNDO**. Se confirma la clasificación de información, en términos de lo expuesto en el considerando II, inciso a), de la presente resolución.*

***TERCERO**. Se revoca la clasificación de información según se expuso en el considerando II, inciso b), de esta determinación.*

***CUARTO**. Se requiere a la Dirección General de Tecnologías de la Información y a la Unidad General de Transparencia y Sistematización de la*

---

incidentes que afecten a la seguridad. Cuando sea posible, estas actuaciones habrán de suponer un intercambio de información y una cooperación transfronteriza.

5) Democracia.

La seguridad de los sistemas y redes de información debe ser compatible con los valores esenciales de una sociedad democrática.

La seguridad debe lograrse de manera consistente con garantía de los valores reconocidos por las sociedades democráticas, incluyendo la libertad de intercambio de pensamiento e ideas, así como el libre flujo de información, la confidencialidad de la información y la comunicación y la protección apropiada de información personal, apertura y transparencia.'

[19] *'**Artículo 37***

Del cumplimiento de las resoluciones

(…)

Cuando el dictamen aprobado por el Comité determine incumplida la resolución, se apercibirá a la instancia respectiva para que, en un plazo no mayor a dos días hábiles, cumpla con la resolución del Comité e informe tal circunstancia al Secretario. Advirtiéndole que en caso de un nuevo incumplimiento se dará vista a la Contraloría de la Suprema Corte…'

x1/iAQw9lPZGQkEmApJv5g8vd+u8zWPKvjVyNm1uO8s=

Información Judicial para que realicen las acciones referidas en la parte final de esta resolución.
[…]"

IV. Requerimiento para actualizar el índice de información reservada. Por oficio CT-618-2023 de seis de octubre de dos mil veintitrés, la Secretaría de este Comité de Transparencia solicitó a la Dirección General de Tecnologías de la Información (DGTI) que se pronunciara sobre la vigencia de la reserva de la información clasificada, o bien, si procedía su desclasificación.

V. Presentación de informe. Al oficio DGTI/500/2023, enviado a través del Sistema de Gestión Documental Institucional el diecinueve de octubre de dos mil veintitrés, la DGTI adjuntó la Nota de Cumplimiento DGTI/DSI-20-2023, a través de la cual informó lo siguiente:

*"**ASUNTO: PRONUNCIAMIENTO SOBRE AMPLIACIÓN DE RESERVA***

Me refiero al oficio número CT-618-2023, fechado el día 6 de octubre del año en curso, a través del cual la Secretaria de Seguimiento del Comité de Transparencia de la Suprema Corte de Justicia de la Nación hizo del conocimiento que conforme a los registros del índice de información reservada con corte a junio de 2023, se encuentra próximo a concluir el plazo de reserva de la información del expediente cumplimiento CT-CUM/A-36/2018 derivado del CT-CI/A-20-2018, por lo que solicitó que, a más tardar el 20 de octubre de 2023, se le informe si el plazo de la reserva es susceptible de ampliarse o si procede la desclasificación. Estos expedientes están relacionados con la siguiente información:

'… (…) ataques cibernéticos que la dependencia federal ha recibido de enero de 2018 a la fecha. Favor de detallar por mes, tipo de ataque y lugar de origen'

Al respecto, se informa que subsisten las causas que dieron origen a la clasificación de la información como reservada, con fundamento en el artículo 110, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública y la fracción I del artículo 113, de la Ley General de Transparencia y Acceso a la Información Pública, como a continuación se expone:

Conforme al artículo 111 de la Ley Federal de Transparencia y Acceso a la Información Pública los sujetos obligados deben fundar y motivar las causales de reserva previstas en el artículo 110 de dicho ordenamiento, 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. Por su parte, el mencionado artículo 104 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.

x1/iAQw9lPZGQkEmApJv5g8vd+u8zWPKvjVyNm1uO8s=

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.´*

Bajo este contexto, debe señalarse que, la normativa establece las causales de reserva y establece como mecanismo para fundar y motivar tales causales, la aplicación de una prueba de daño que deben proporcionar los sujetos obligados para acreditarse el cumplimiento de elementos que se señalan en el Trigésimo Tercero de los Lineamientos Generales.

Por su parte, el artículo 99 de la Ley Federal de Transparencia y Acceso a la Información Pública prevé la posibilidad para los sujetos obligados de ampliar el plazo de reserva siempre y cuando justifiquen que subsisten las causas que dieron origen a su clasificación, mediante la aplicación de una prueba de daño.

Por lo anterior, a fin de fundar y motivar la ampliación del periodo de reserva de la información, se informa que subsisten las causas que dieron origen a la clasificación de la información, por lo que se aplica la siguiente prueba de daño:

> ➢ *Existe un riesgo real, demostrable e identificable de perjuicio significativo al interés público que colocaría a la Suprema Corte de Justicia de la Nación en un estado de vulnerabilidad, ya que al dar a conocer el tipo y el lugar de origen de los ataques cibernéticos implicaría:*
>
> - *Capacidad para identificar la versión de firmware del equipo de seguridad, con lo cual podrían explotar una vulnerabilidad y modificar sin autorización los portales electrónicos de la SCJN.*
> - *Recepción de ataques no recibidos o identificados en la infraestructura de seguridad informática, llegando a afectar el contenido de los portales electrónicos.*

x1/iAQw9lPZGQkEmApJv5g8vd+u8zWPKvjVyNm1uO8s=

- *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 de internet de la SCJN.*
- *Facilitar la extracción, modificación o alteración de información sensible de los expedientes jurisdiccionales, lo que incidiría directa y negativamente en la tarea sustantiva de este Alto Tribunal, y por otra parte, comprometería la información administrativa, que actualizaría un riesgo a las personas en lo particular, tales como trabajadores y proveedores, al hacerse patente un acceso no autorizado, ni controlado a los datos personales que se tengan registrados, e inclusive información contable o bancaria, por solo citar algunos casos.*

➢ *Se supera el interés público general de que se difunda la información, ya que el resguardo de los datos consistentes en tipo y el lugar de origen de los ataques cibernéticos implica proteger a la SCJN de un reconocimiento del tipo de ataques cibernéticos que se han recibido y mitigado en los portales de internet, asimismo, se salvaguardan los lugares de origen de esos ciberataques, al carecer de un filtrado de peticiones que,*
de no resguardarse, pondría en riesgo la infraestructura de los portales electrónicos de la SCJN.

➢ *El proteger la información clasificada como reservada se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio, toda vez que la pretensión de fondo que persigue el que la información continue siendo reservada deriva de que con la divulgación se puede proporcionar información de la operación y seguridad de los servicios publicados en internet de la SCJN, para evitar ataques informáticos, afectación y degradación de los servicios de información, que de revelarse 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. Adicional a lo anterior, 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.*

En conclusión, es procedente ampliar la reserva de la información, ya que subsisten las causas que dieron origen a su clasificación, con fundamento en los artículos 99, tercer párrafo y 110, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública y la fracción I del artículo 113, de la Ley General de Transparencia y Acceso a la Información Pública.

Ahora bien, en cuanto al periodo de reserva, el mencionado 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 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.

Por otra parte, el tercer párrafo del artículo 99 antes mencionado señala:

x1/iAQw9lPZGQkEmApJv5g8vd+u8zWPKvjVyNm1uO8s=

'Artículo 99. (…)
Fracciones I a V (…)
(…)
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.
(…)'

En el caso concreto, considerando la aplicación de la prueba de daño, se justifica que prevalecen las causas que originaron la reserva y por ello el periodo debe ampliarse hasta por un plazo de cinco años adicionales.

Sirve para reforzar lo anterior, lo expuesto a través de la resolución del expediente cumplimiento CT-CUM/A-36/2018, derivado del diverso CT-CI/A-20-2018[20], emitida por el Comité de Transparencia de la Suprema Corte de Justicia de la Nación, misma que señala lo siguiente:

*'…IV. Respuesta en relación a la resolución del Comité de Transparencia. En respuesta al requerimiento formulado por este Comité de Transparencia, el Director General de Tecnologías de la Información, por oficio DGTI/DAPTI-1999-2018, recibido el veintiuno de septiembre del presente año, adjuntó como anexo un **documento que da cuenta de la prueba de daño en el siguiente sentido**:*
…

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.*	• *Aumento de ataques informáticos específicos contra las versiones y marca de los equipos de seguridad informática identificados.* • *Capacidad para identificar la versión*
Escenario	*Implicación*	*Daño o afectación*
	Reconocimiento del tipo de ataques web que se han recibido y mitigado en los portales web	*firmware del equipo de seguridad, con lo cual podrían explotar una vulnerabilidad y modificar sin autorización los portales web de la SCJN.* • *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 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*

[20] *Disponible para consulta en: […]*

x1/iAQw9lPZGQkEmApJv5g8vd+u8zWPKvjVyNm1uO8s=

		de los portales web de la SCJN.

Conforme a esto, el Director General de Tecnologías de la Información, sin precisar causal de reserva alguna, a grandes rasgos dijo que la divulgación de los datos solicitados podría exponer la capacidad de reacción de los sistemas de seguridad informáticos y propiciar el aumento y especificidad de ataques cibernéticos, al proporcionar información sensible de la operación y seguridad de los servicios publicados en Internet de este Alto Tribunal, ya que implicaría lo siguiente:

…

- *Sobre 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;*
- *Del lugar, 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.*

Con lo anterior, se tiene que se ha dado cumplimiento a lo ordenado por este órgano colegiado, por parte de la instancia requerida, correspondiendo ahora realizar el estudio concreto de la clasificación de información. Así, dada la motivación que da el área, ***se arriba a la conclusión que, en su caso y como se verá, pesaría la reserva establecida en la fracción I, del artículo 113, de la Ley General****, que establece lo siguiente:*

*‘**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;…**’*

Esto porque, 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****, 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.*

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

…se tiene que la Dirección General de Tecnologías de la Información es la área técnica [sic] *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 por el artículo 27, fracción I, del Reglamento Orgánico en Materia Administrativa de la Suprema Corte de Justicia de la Nación.*

En ese sentido, tratándose de cuestiones que atañen a la protección específica de los rubros que involucran aspectos vinculados con la infraestructura se seguridad informática 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/o valorar la razonabilidad de la clasificación expresada para efecto de su confirmación o no.

Precisado lo anterior, ***corresponde ahora analizar,*** *desde la razonabilidad de la motivación expresada por el área,* ***si los datos específicamente requeridos (número, tipo y lugar de origen de los ataques cibernéticos que se hubieren presentado en esta Suprema Corte de Justicia de la Nación) darían lugar o no a la clasificación total de la información solicitada.***

a) Tipo y lugar de origen de los ataques cibernéticos*. Por cuanto estos datos, ante la razón desprendida de los informes presentados por el área requerida y responsable,* ***este Comité de Transparencia identifica, como se ha venido señalando, que se pretende proteger, desde un esquema global, la infraestructura de seguridad informática de este Alto Tribunal, en***

x1/iAQw9lPZGQkEmApJv5g8vd+u8zWPKvjVyNm1uO8s=

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, e inclusive información contable o bancaria, por solo citar algunos casos.

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 relaciona su valoración.*

Lo anterior, porque, ***se podrían poner en riesgo cuestiones de seguridad pública, pues según se refirió previamente, a partir de la información solicitada, si se divulgara, 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, como se anunciaba previamente, lo que ***se impone es confirmar la determinación del área, para efecto de confirmar la reserva de la información solicitada****, por un plazo de cinco años en atención a lo establecido por el artículo 1018, de la Ley General."*

Así como lo señalado por la resolución dentro del expediente CT-CI/A-2-20212, de fecha veintisiete de enero de dos mil veintiuno, la cual señala:

*'**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 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.

-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 CTCUM/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,***

x1/iAQw9lPZGQkEmApJv5g8vd+u8zWPKvjVyNm1uO8s=

> ***comprende garantizar el buen funcionamiento de los sistemas de seguridad informáticos ante posibles ataques cibernéticos , 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.*
>
> *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(directrices), de la OCDE (por sus siglas en inglés: Organisation for Economic Cooperation and Development)'.* [sic]
> *…*
> *De manera similar a* ***lo argumentado en la resolución CT-CUM/A36-2018****, 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.*** *…*
> *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 1018 de la Ley General de Transparencia.*
> *[...]"*

VI. Acuerdo de turno. Mediante acuerdo de diecinueve de octubre de dos mil veintitrés, el Presidente del Comité de Transparencia ordenó su remisión al Director General de Asuntos Jurídicos de esta Suprema Corte de Justicia de la Nación, en su carácter de 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 de Transparencia), y 23, fracción II, y 27 del Acuerdo General de Administración 5/2015.

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

x1/iAQw9lPZGQkEmApJv5g8vd+u8zWPKvjVyNm1uO8s=

I. Competencia. El Comité de Transparencia de la Suprema Corte de Justicia de la Nación es competente para resolver sobre la ampliación del periodo de reserva de la información, de conformidad con los artículos 6° de la Constitución Política de los Estados Unidos Mexicanos; 44, fracción VIII, y 101, párrafo tercero, de la Ley General de Transparencia; 65, fracción VIII, y 99, párrafo tercero, de la Ley Federal de Transparencia y Acceso a la Información Pública (Ley Federal de Transparencia); 23, fracción I, y 37 del Acuerdo General de Administración 5/2015.

II. Análisis. Como se advierte del antecedente I, en la solicitud se requirió diversa información sobre ataques cibernéticos recibidos del uno de enero al cinco de julio de dos mil dieciocho; sin embargo, en la resolución del expediente CT-CI/A-20-2018 se consideró que la DGTI debía precisar y justificar desde la prueba de daño la reserva de la información solicitada, de acuerdo con la causal o hipótesis respectiva, de las encausadas en artículo 113 de la Ley General de Transparencia.

Al efecto, la respuesta de dicha área se analizó en la resolución del expediente **CT-CUM/A-36/2018** en los siguientes términos:

- Se expuso que, si bien en el informe de la DGTI no se precisó causal de reserva alguna, a grandes rasgos se dijo que la divulgación de los datos solicitados podría exponer la capacidad de reacción de los sistemas de seguridad informáticos y propiciar el aumento y especificidad de ataques cibernéticos, al proporcionar información sensible de la operación y seguridad de los servicios publicados en Internet de este Alto Tribunal.
- En consecuencia, dada la motivación del área, se arribó a la conclusión de que, en su caso, pesaría la reserva establecida en la **fracción I, del artículo 113, de la Ley General de Transparencia** porque, desde una óptica general, el objeto de la restricción de la información, comprende garantizar el buen funcionamiento de los sistemas de seguridad informáticos ante posibles ataques cibernéticos que, en general pondrían en riesgo la información de este Alto Tribunal (tanto del quehacer jurisdiccional como administrativo) y, ello daría lugar a su posible extracción, modificación o alteración, lo que en última instancia comprometería el ejercicio de los derechos de las personas (acceso a la justicia).

x1/iAQw9lPZGQkEmApJv5g8vd+u8zWPKvjVyNm1uO8s=

- Aunado a que es imperante que se cuente 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 de la Organización para la Cooperación y el Desarrollo Económicos (OCDE).
- Una vez identificada la causal de reserva, se indicó que es competencia del titular de la instancia que tiene bajo su resguardo la información requerida, determinar su disponibilidad y clasificarla conforme a los criterios establecidos en la normativa aplicable
- Se precisó que la DGTI 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.
- Tratándose de cuestiones que atañen a la protección específica de los rubros que involucran aspectos vinculados con la infraestructura se seguridad informática del Alto Tribunal, cuando el área enteramente responsable ubica el surgimiento de elementos que inciden en la dimensión ya señalada, el órgano encargado de conocer del acceso solo debe limitarse a entender y/o valorar la razonabilidad de la clasificación expresada para efecto de su confirmación o no.
- Se analizó desde la razonabilidad de la motivación expresada por el área, si los datos específicamente requeridos (número, tipo y lugar de origen de los ataques cibernéticos que se hubieren presentado en esta Suprema Corte de Justicia de la Nación) darían lugar o no a la clasificación total de la información solicitada.
- Respecto al **tipo y lugar de origen de los ataques cibernéticos** se sostuvo que:
    - De los informes presentados por el área requerida se identificó 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, la extracción, modificación o alteración de información de los expedientes jurisdiccionales y, por otra parte, un probable riesgo a las personas en lo particular como son trabajadores y proveedores, al

x1/iAQw9lPZGQkEmApJv5g8vd+u8zWPKvjVyNm1uO8s=

hacerse patente un acceso no autorizado ni controlado a información administrativa.

- La clasificación advertida también se sustentó, desde la prueba de daño, porque se podrían poner en riesgo cuestiones de seguridad pública, pues a partir de la información solicitada, si se divulgara, 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 sí pesa sobre la capacidad de respuesta.
- El plazo de clasificación de determinó por cinco años.

- Respecto al **número de ataques cibernéticos** se consideró factible dar a conocer, de forma global, el número de ataques cibernéticos que había recibido este Alto Tribunal del uno de enero al cinco de julio de dos mil dieciocho; en consecuencia, se revocó la clasificación efectuada por la DGTI con relación ese dato y, se requirió que remitiera a la Unidad General de Transparencia el informe correspondiente.

Ahora, considerando el vencimiento del plazo de reserva de la información y, de acuerdo con lo resuelto por el Comité de Transparencia en el asunto CT-CUM/A-36/2018, la Secretaría de este órgano colegiado solicitó a la DGTI que emitiera un informe en el que señalara si las causas de reserva prevalecían o no. En consecuencia, dicha instancia informó lo siguiente:

- Subsisten las causas que dieron origen a la clasificación de la información como reservada, con fundamento en los artículos **110, fracción I,** de la Ley Federal de Transparencia y **113, fracción I**, de la Ley General de Transparencia.

- Existe un riesgo real, demostrable e identificable de perjuicio significativo al interés público que colocaría a la Suprema Corte de

x1/iAQw9lPZGQkEmApJv5g8vd+u8zWPKvjVyNm1uO8s=

Justicia de la Nación en un estado de vulnerabilidad, ya que dar a conocer el tipo y el lugar de origen de los ataques cibernéticos implicaría:

- Capacidad para identificar la versión de *firmware* del equipo de seguridad, con lo cual podrían explotar una vulnerabilidad y modificar sin autorización los portales electrónicos del Máximo Tribunal.
- Recepción de ataques no recibidos o identificados en la infraestructura de seguridad informática, llegando a afectar el contenido de los portales electrónicos.
- Aumento de ataques informáticos desde regiones o zonas donde se tiene permitido el flujo de tráfico hacia los portales de internet institucionales, lo que agotaría el enlace de comunicación de los portales de internet del Alto Tribunal.
- Facilitar la extracción, modificación o alteración de información de los expedientes jurisdiccionales, lo que incidiría directa y negativamente en la tarea sustantiva de este Alto Tribunal y, por otra parte, comprometería la información administrativa, que actualizaría un riesgo a las personas en lo particular, tales como trabajadores y proveedores, al hacerse patente un acceso no autorizado, ni controlado a los datos personales que se tengan registrados, e inclusive información contable o bancaria, por solo citar algunos casos.

- Se supera el interés público general de que se difunda la información, ya que el resguardo de los datos consistentes en tipo y el lugar de origen de los ataques cibernéticos implica proteger a la Suprema Corte de Justicia de la Nación de un reconocimiento del tipo de ataques cibernéticos que se han recibido y mitigado en los portales de internet; asimismo, se salvaguardan los lugares de origen de esos ciberataques, al carecer de un filtrado de peticiones que, de no resguardarse, pondría en riesgo la infraestructura de los portales electrónicos del Alto Tribunal.

- El proteger la información clasificada como reservada se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio, toda vez que la pretensión de fondo que persigue el que la información continue siendo reservada deriva de

x1/iAQw9lPZGQkEmApJv5g8vd+u8zWPKvjVyNm1uO8s=

que con la divulgación se puede proporcionar información de la operación y seguridad de los servicios publicados en internet de la Suprema Corte de Justicia de la Nación, para evitar ataques informáticos, afectación y degradación de los servicios de información, que de revelarse 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.

- En cuanto al periodo de reserva, para el caso concreto, considerando la aplicación de la prueba de daño, se justifica que prevalecen las causas que originaron la reserva y, por ello, el periodo debe ampliarse hasta por un plazo de cinco años adicionales.

Para analizar la ampliación del plazo de reserva que solicita la DGTI se tiene presente que en términos de los artículos 100[21] de la Ley General de Transparencia y 97[22] de la Ley Federal de Transparencia, en relación con el artículo 17[23] del Acuerdo General de Administración 5/2015, las personas titulares de las instancias

[21] "**Artículo 100.** La clasificación es el proceso mediante el cual el sujeto obligado determina que la información en su poder actualiza alguno de los supuestos de reserva o confidencialidad, de conformidad con lo dispuesto en el presente Título.
Los supuestos de reserva o confidencialidad previstos en las leyes deberán ser acordes con las bases, principios y disposiciones establecidos en esta Ley y, en ningún caso, podrán contravenirla.
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."

[22] "**Artículo 97.** La clasificación es el proceso mediante el cual el sujeto obligado determina que la información en su poder actualiza alguno de los supuestos de reserva o confidencialidad, de conformidad con lo dispuesto en el presente Título.
En el proceso de clasificación de la información, los sujetos obligados observarán, además de lo establecido en el Título Sexto de la Ley General, las disposiciones de la presente Ley.
Los titulares de las Áreas de los sujetos obligados serán los responsables de clasificar la información, de conformidad con lo dispuesto en la Ley General y la presente Ley.
Los sujetos obligados deberán aplicar, de manera restrictiva y limitada, las excepciones al derecho de acceso a la información previstas en el presente Título y deberán acreditar su procedencia, sin ampliar las excepciones o supuestos de reserva o confidencialidad previstos en las leyes, de conformidad con lo establecido en la Ley General.
Los sujetos obligados no podrán emitir acuerdos de carácter general ni particular que clasifiquen documentos o expedientes como reservados, ni clasificar documentos antes de dar respuesta a una solicitud de acceso a la información.
La clasificación de información reservada se realizará conforme a un análisis caso por caso, mediante la aplicación de la prueba de daño."

[23] "**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.
A efecto de instituir un vínculo de comunicación para las gestiones derivadas de trámites de acceso a la información, protección de información reservada y/o confidencial y transparencia, los titulares de las instancias designarán un servidor público que fungirá como Enlace e informarán por escrito sobre su designación a la Unidad General."

x1/iAQw9lPZGQkEmApJv5g8vd+u8zWPKvjVyNm1uO8s=

que tienen bajo resguardo la información solicitada son las responsables de determinar su disponibilidad y clasificarla conforme a la normativa aplicable.

En el caso concreto, la DGTI es el área técnica que cuenta con el personal especializado para velar por la seguridad de la información de los sistemas tecnológicos del Alto Tribunal, en virtud de que el artículo 36[24] del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación prevé como una de sus atribuciones la de administrar los sistemas informáticos jurídicos, administrativos y jurisdiccionales de este Alto Tribunal.

x1/iAQw9lPZGQkEmApJv5g8vd+u8zWPKvjVyNm1uO8s=

[24] "**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;
II. Recabar las necesidades de bienes y servicios en materia de tecnologías de la información y comunicación que requieran los órganos y áreas, así como dictaminar sobre sus características técnicas y sobre la procedencia, así como gestionar su incorporación en el programa anual de necesidades que corresponda;
III. Proporcionar a la Dirección General de Presupuesto y Contabilidad la información presupuestaria derivada de las necesidades de bienes y servicios en materia de tecnologías de la información y comunicación, para el proceso de elaboración del Proyecto de Presupuesto de Egresos de la Suprema Corte;
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;
VI. Elaborar estudios técnicos en materia de infraestructura tecnológica, así como de sistemas y bienes informáticos;
VII. Operar el centro de atención a usuarios y soporte técnico para la resolución de los requerimientos en materia de tecnologías de la información y comunicación;
VIII. Proporcionar los servicios de mantenimiento a las redes, equipo informático, comunicación y digitalización de los órganos y áreas de la Suprema Corte y, en su caso, a otros órganos del Poder Judicial de la Federación;
IX. Instrumentar los mecanismos en materia de seguridad informática y vigilar su adecuado funcionamiento;
X. Colaborar con la Dirección General de Recursos Materiales en la actualización del inventario de los bienes informáticos de la Suprema Corte;
XI. Proporcionar la información y, en su caso, la asesoría necesaria para el aseguramiento de los bienes informáticos y de comunicaciones, así como de las reclamaciones a las instituciones de seguros en caso de siniestros ocurridos;
XII. Implementar tecnológicamente la estrategia de gobierno de datos que regula el uso, gestión y explotación de éstos;
XIII. Emitir el dictamen resolutivo técnico de las propuestas presentadas por los participantes en los diferentes procedimientos de contratación de adquisición de bienes y servicios de carácter informático;
XIV. Suscribir, en el ámbito de su competencia, los contratos y convenios relacionados con la adquisición de bienes y servicios informáticos, de conformidad con las disposiciones jurídicas aplicables, y
XV. Actuar como Unidad Responsable Integradora, en el ámbito de su competencia, así como verificar y registrar las operaciones en el Sistema Integral Administrativo, en términos de las disposiciones jurídicas aplicables."

Con base en lo anterior, la DGTI ha informado que en términos del artículo 113, fracción I, de la Ley General de Transparencia **subsiste** el riesgo real, demostrable e identificable que originó que se reservará la información requerida en la solicitud de origen, en relación con el **tipo y lugar de origen de los ataques cibernéticos** recibidos en este Alto Tribunal en periodo del uno de enero al cinco de julio de dos mil dieciocho.

Ahora, a pesar de que en el cumplimiento CT-CUM/A-36-2018 la clasificación fue confirmada con fundamento en el artículo 113, fracción I, de la Ley General de Transparencia, y de que la instancia responsable expone que subsisten las causas que dieron origen a dicha clasificación, a partir de una nueva reflexión, en diversos asuntos[25] este órgano colegiado ha determinado clasificar información similar y, bajo argumentos equivalentes, con fundamento en la fracción VII del propio artículo 113 de la Ley General de Transparencia.

En tal contexto, se tiene en consideración que las razones expuestas para motivar la ampliación del plazo de reserva se refieren a que la divulgación de esa información implicaría proporcionar elementos de la operación y seguridad de los servicios publicados en internet del Máximo Tribunal, por lo que de revelarse podrían aumentar los **ataques** informáticos, inclusive de aquellos no recibidos o identificados previamente y, se permitiría que se incremente el número de ataques desde regiones o zonas donde se tiene permitido el flujo tráfico hacia los portales de internet de esta Suprema Corte de Justicia de la Nación.

En ese sentido, la información relativa al tipo y lugar de origen de los ataques cibernéticos recibidos en el Alto Tribunal en el periodo comprendido entre el uno de enero y el cinco de julio de dos mil dieciocho, constituye información susceptible de mantenerse clasificada como reservada, en tanto que la instancia

[25] CT-CI/A-16-2023. Se clasificaron el número de serie y/o direcciones *MAC* (por sus siglas en inglés *Media Access Control*) de los equipos de cómputo de este Alto Tribunal. Disponible en: CT-VT/A-16-2023 (scjn.gob.mx)
CT-VT/A-29-2023. Se clasificó información contenida en el código fuente utilizado en la página de un buscador jurídico. Disponible en: CT-VT-A-29-2023.pdf (scjn.gob.mx)
CT-VT/A-22-2023. Se clasificó información relativa a código fuente y algoritmos del software. Disponible en: CT-VT-A-22-2023.pdf (scjn.gob.mx)

x1/iAQw9IPZGQkEmApJv5g8vd+u8zWPKvjVyNm1uO8s=

vinculada informa que se refiere a aspectos vinculados con la **seguridad técnica** de los sistemas tecnológicos de este Máximo Tribunal y, que podría atentar contra la operación y seguridad de los servicios publicados en el portal de internet de la Suprema Corte de Justicia de la Nación.

Además, 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 a un estado de **vulnerabilidad**, en tanto se pondría en riesgo la infraestructura de los portales electrónicos de este Alto Tribunal.

En consecuencia, se estima que las razones convergen en la actualización de la causal prevista en la fracción VII del artículo 113 de la Ley General de Transparencia, de cuyo contenido se desprende que se podrá clasificar como información reservada aquella cuya publicación obstruya la prevención o persecución de los delitos[26].

Como apoyo a tal conclusión se retoma, en lo que interesa, lo que el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) sostuvo al resolver el recurso de revisión 10276/18[27]:

> *"[…]*
> *Por todo lo anterior, se advierte que **difundir** información relativa a los números de serie de los equipos y la versión del firewall instalado, **incrementa sustancialmente la posibilidad de que aquella persona que conozca dicha información cometa algún ilícito**, accediendo de forma no autorizada a los sistemas de datos que no son públicos en posesión del sujeto obligado, conociendo con un alto grado de precisión la información técnica referente a sus equipos de cómputo, los protocolos de seguridad y las características de la infraestructura instalada.*
>
> *En esa tónica, derivado de la naturaleza y el grado de especificidad del tipo de información que se requiere, y que se trata de un elemento relevante al ponderar cualquier posible vulneración a la seguridad de la infraestructura tecnológica de la autoridad obligada, es que se colige que dar a conocer la misma facilitaría que*

[26] "**Artículo 113.** Como información reservada podrá clasificarse aquella cuya publicación:
[…]
VII. Obstruya la prevención o persecución de los delitos;
[…]"
[27] Resuelto el 20 de febrero de 2019. Consultable en: consultas.ifai.org.mx/Sesiones

x1/iAQw9lPZGQkEmApJv5g8vd+u8zWPKvjVyNm1uO8s=

> *personas expertas en informática **perturben el sistema de la infraestructura tecnológica** de la Suprema Corte de Justicia de la Nación, ejecuten programas informáticos perjudiciales que modifiquen o destruyan información relevante; situación que pondría en un estado vulnerable la información que en ella se contiene, facilitando la intervención de las comunicaciones y permitiendo usurpar permisos requeridos en la red para obtener información; resultando, por lo tanto, es procedente su reserva, de conformidad con el precepto jurídico que se analiza.*
>
> *Es decir, este Organismo Garante del derecho de acceso a la información pública concluye que **procede la reserva** de la información relativa al número de serie, el conocer si los discos duros se encuentran encriptados, el nombre comercial de los programas de encriptado de información, conocer si pueden borrar o no archivos con o sin contraseñas y conocer si se puede almacenar información a través de los puertos USB, de cada uno de los equipos de cómputo en posesión del sujeto obligado, de conformidad con lo previsto en el artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.*
> *[…]"*

Así, este Comité concluye que las razones respecto de las cuales el INAI precisó que se actualizaba la fracción VII, del artículo 110, de la Ley Federal de Transparencia[28] (de contenido idéntico a la diversa VII del artículo 113 de la Ley General de Transparencia), son coincidentes con las expuestas por la instancia vinculada para motivar la ampliación del plazo de reserva de la información, en virtud de que confluyen en la posibilidad de una vulneración a la seguridad de la **infraestructura** tecnológica de este Alto Tribunal (portales electrónicos), así como en facilitar la **extracción**, **modificación** o **alteración** de información relevante.

Por cuanto hace a la prueba de daño y en concordancia con los argumentos señalados, se estima que subsisten las causas que dieron origen a la clasificación de la información relativa al tipo y lugar de origen de los ataques cibernéticos recibidos en este Alto Tribunal en el periodo comprendido entre el uno de enero y el cinco de julio de dos mil dieciocho.

A mayor abundamiento, se retoma lo manifestado en la resolución CT-CUM-R/A-2-2019[29]: *"como información reservada podrá clasificarse aquella cuya*

x1/iAQw9lPZGQkEmApJv5g8vd+u8zWPKvjVyNm1uO8s=

---

[28] **Ley Federal de Transparencia**
"**Artículo 110.** Como información reservada podrá clasificarse aquella cuya publicación:
VII. Obstruya la prevención o persecución de los delitos;
[…]"

[29] Derivada del recurso de revisión 10276/18 ya citado. Disponible en: CT-CUM-R-A-2-2019.pdf (scjn.gob.mx)

publicación obstruya la prevención o persecución de delitos", agregando que "para que pueda acreditarse que la información requerida pudiera 'obstruir la prevención de los delitos', debe vincularse a la afectación a las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de las autoridades para evitar la comisión de delitos"; además, se agregó que *"para que pueda acreditarse que la información requerida pudiera 'obstruir la prevención de los delitos', debe vincularse a la afectación a las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de las autoridades para evitar la comisión de delitos".*

De igual manera se precisó que, *de esa causal de reserva se desprenden dos vertientes: una que se refiere a la prevención de los delitos y la otra a la persecución de los mismos, […] "'por definición de la palabra prevención se hace referencia a medidas y acciones dispuestas con anticipación con el fin de evitar o impedir que se presente un fenómeno peligroso para reducir sus efectos sobre la publicación', de ahí que 'prevención del delito' significa 'tomar medidas y realizar acciones para evitar una conducta o un comportamiento que puedan dañar o convertir a la población en sujetos o víctimas de un ilícito' y que desde el punto de vista criminológico prevenir es 'conocer con anticipación la probabilidad de una conducta criminal disponiendo de los medios necesarios para evitarla; es decir, no permitir que alguna situación llegue a darse porque ésta se estima inconveniente'.*

Igualmente se hizo alusión al Código Penal Federal en los términos siguientes: "comete el ***delito de acceso ilícito a sistemas y equipos de informática*** *todo aquel que* ***sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad****, sean o no propiedad del Estado. Asimismo, al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa".*

x1/iAQw9lPZGQkEmApJv5g8vd+u8zWPKvjVyNm1uO8s=

Por consiguiente, en términos del artículo 104 de la Ley General de Transparencia[30] se concluye que, el daño que podría producirse con la publicidad de la información es mayor que el interés de conocerla, pues como se dijo, a partir del tipo y lugar de origen de los ataques cibernéticos se podría poner en riesgo la infraestructura de los portales electrónicos; asimismo, se facilitaría la extracción, modificación o alteración de información relevante, lo que incidiría directa y negativamente en la tarea sustantiva de este Alto Tribunal y, por otra parte, se podría comprometer la información administrativa.

En consecuencia, de conformidad con los artículos 44, fracción VIII, y 103 de la Ley General de Transparencia, se determina justificado ampliar el plazo de reserva respecto del tipo y lugar de origen de los ataques cibernéticos recibidos en este Alto Tribunal; no obstante, el fundamento es el artículo **113, fracción VII**, de la Ley General de Transparencia.

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 de clasificación.

Por lo expuesto y fundado; se,

R E S U E L V E:

x1/iAQw9lPZGQkEmApJv5g8vd+u8zWPKvjVyNm1uO8s=

[30] “**Artículo 104.** En la aplicación de la prueba de daño, el sujeto obligado deberá justificar que:
I. La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público o a la seguridad nacional;
II. El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda, y
III. La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio.”

ÚNICO. Se confirma la ampliación del plazo de reserva de la información en los términos de la presente resolución.

Notifíquese 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 licenciado Mario José Pereira Meléndez, Director General de Asuntos Jurídicos y Presidente del Comité, maestro Christian Heberto Cymet López Suárez, Contralor del Alto Tribunal, y licenciado Adrián González Utusástegui, Titular de la Unidad General de Investigación de Responsabilidades Administrativas; quienes firman con 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

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."

x1/iAQw9lPZGQkEmApJv5g8vd+u8zWPKvjVyNm1uO8s=