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

CT-CUM/A-29-2026 derivado del expediente CT-VT/A-31-2026

INSTANCIAS REQUERIDAS:

- DIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA UNIDAD DE ADMINISTRACIÓN DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN
- DIRECCIÓN GENERAL DE PRESUPUESTO Y CONTABILIDAD DE LA UNIDAD DE ADMINISTRACIÓN DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN

Ciudad de México. Resolución del Comité de Transparencia de la Suprema Corte de Justicia de la Nación, correspondiente a la sesión del **dos de julio de dos mil veintiséis**.

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

PRIMERO. Solicitud de información. El trece de abril de dos mil veintiséis, se realizó una solicitud de acceso a la información, a través de la Plataforma Nacional de Transparencia con el folio **1550030526000638**, mediante la cual se requirió lo siguiente:

> "Solicito la siguiente información pública, correspondiente al periodo comprendido del 1 de enero de 2007 al 13 de abril de 2026, relacionada con incidentes de ciberseguridad, filtraciones de información, capacidades institucionales y acciones implementadas:
>
> 1. El número total de incidentes de ciberseguridad registrados por la dependencia, desagregado por año desde el 1 de enero de 2007 al 13 de abril de 2026
> […]
>
> 6. Solicito, desagregado por año:
> […]
> ● Presupuesto destinado a ciberseguridad
>
> 7. Solicito:
> ● Protocolos de atención a incidentes de ciberseguridad
> […]" (*sic*)[1]

[1] Se transcriben únicamente las partes que nos ocupan para efectos de analizar el cumplimiento en la presente resolución.

wwExGMIPGUgDIkUQPBDb9Raz3XelybeA5N2TDQTwNd0=

SEGUNDO. Resolución del Comité de Transparencia de la Suprema Corte de Justicia de la Nación. En sesión de veintiocho de mayo de dos mil veintiséis, el Comité de Transparencia emitió resolución en el expediente **CT-VT/A-31-2026**, en la cual, en la parte conducente, se determinó lo siguiente:

"[…]

II.- Información pendiente

- **Punto 6, inciso c)**

En este apartado, es necesario recordar que, respecto del **punto 6** inciso **c)**, la **DGPC** informó que la Suprema Corte de Justicia de la Nación como ejecutora de gasto, registra y reporta la información presupuestaria conforme al Clasificador por Objeto del Gasto, que desagrega los recursos por capítulo, concepto y partida presupuestaria, por lo que para los ejercicios de dos mil veinte a dos mil veintiséis, "no se cuenta con la información".

Además, informó que los expedientes presupuestales y contables de dos mil diecinueve y anteriores, concluyeron con su ciclo archivístico, por lo que se procedió con la baja documental.

En seguimiento a lo anterior, se desprende que, si bien, proporcionó el vínculo electrónico que remite al Clasificar por Objeto del Gasto, lo cierto es que fue omiso en dar cumplimiento al artículo 132[2] de la Ley General de Transparencia, pues no indicó los pasos a seguir para acceder al capítulo, concepto o partida presupuestaria que se relacionen, en su caso, con la materia de la solicitud, es decir, a los datos que pudieran dar cuenta del gasto por concepto de ciberseguridad o, en su defecto, explicar por qué no cuenta con la información específica de interés de la persona solicitante, dado que únicamente señala que "no se cuenta" con ella, y que se toma en consideración lo establecido en el artículo 131 de la Ley General de Transparencia.

Por otro lado, respecto de los años dos mil siete a dos mil diecinueve, si bien la **DGPC** señaló que los expedientes presupuestales y contables concluyeron con su ciclo archivístico, por lo que fue procedente su baja documental, lo cierto es que fue **omisa** en proporcionar la expresión documental en la que conste la referida baja, para otorgar certeza jurídica a la persona solicitante de la inexistencia manifestada.

En ese sentido, considerando que este Comité de Transparencia es competente para dictar las medidas conducentes para la localización de la información bajo resguardo de las instancias de esta Suprema Corte de Justicia de la Nación, con apoyo en los artículos 40, fracción I, de la Ley General de Transparencia, 23, fracciones II y III, y 37 del Acuerdo General de Administración 05/2015[3], por conducto de la Secretaría de este Comité, se **requiere** a la **DGPC**, para que en el término de **cinco** días hábiles siguientes a la notificación de la presente resolución:

- Realice una búsqueda exhaustiva y razonable respecto de los registros que den cuenta de la baja documental de la información solicitada respecto de los años dos mil siete a dos mil diecinueve, relacionada con lo requerido en el

[2] **Artículo 132.** Cuando la información requerida por la persona solicitante ya esté disponible al público en medios impresos, tales como libros, compendios, trípticos, registros públicos, en formatos electrónicos disponibles en Internet o en cualquier otro medio, se le hará saber por el medio requerido por la persona solicitante la fuente, **el lugar y la forma** en que puede consultar, reproducir o adquirir dicha información en un plazo no mayor a cinco días. [**El resaltado es propio**].

[3] "Artículo 23 Atribuciones del Comité
Son atribuciones del Comité, además de las señaladas en el Ley General, las siguientes:
[…]
II. Confirmar, modificar o revocar las determinaciones de las instancias en las que se señale que la información solicitada es inexistente, confidencial o reservada. El Comité cuidará que la información entregada por las instancias se ajuste con precisión a los términos en los cuales se recibió la solicitud;
III. Dictar las medidas conducentes para la localización de información bajo resguardo de las instancias, ordenar su generación o reposición en los términos del artículo 138 fracción III de la Ley General y, en su caso, confirmar su inexistencia;"

wwExGMIPGUgDIkUQPBDb9Raz3XelybeA5N2TDQTwNd0=

punto 6 inciso **c)** de la solicitud, e informe a este órgano colegiado el resultado de dicha búsqueda.

- Se pronuncie fundada y motivadamente con relación a la inexistencia planteada en su informe en atención al artículo 131 la Ley General de Transparencia, respecto del "presupuesto designado al concepto de ciberseguridad", respecto de los ejercicios de dos mil veinte a dos mil veintiséis, del **punto 6** inciso **c)** de la solicitud.

- **Punto 1 (número de incidentes)**

Respecto del **punto 1**, solo en lo que corresponde al: "número total de incidentes de ciberseguridad registrados por la dependencia, desagregado por año…"" (sic), es necesario recordar que, en la resolución del expediente CT-CI/A-2-2021[4], la propia **DGTI** se pronunció respecto del número de intentos o ataques cibernéticos, inclusive, desglosándolos por mes.

En virtud de lo anterior, este Comité **requiere** a la **DGTI** para que en el término de **cinco** días hábiles siguientes a la notificación de la presente resolución envíe a la Unidad de Transparencia lo siguiente:

- Información meramente **estadística** con respecto al **número** total de incidentes de ciberseguridad en el periodo solicitado, que va del uno de enero de dos mil siete al trece de abril de dos mil veintiséis.

- **Punto 7, inciso a) (Protocolo de Atención a Incidentes Mayores de Seguridad Informática)**

No pasa desapercibido que la **DGTI**, al rendir su informe, señaló que en atención al **punto 7** inciso **a)** cuenta con la versión pública del "Protocolo de Atención a Incidentes Mayores de Seguridad Informática", al respecto, se advierte que de la revisión a dicha la versión pública, la información testada en carácter de reservada, se ha aplicado en términos del artículo 112, fracciones I y XVI, sin embargo, del estudio vertido en la presente resolución, se estima que las fracciones aplicables al caso en concreto, son la VII y la XVI del referido artículo 112 de la Ley General de Transparencia, por lo que la versión pública proporcionada no resulta procedente; razón por la cual, por conducto de la Secretaría de este Comité, se **requiere** a la **DGTI**, para que en el término de **cinco** días hábiles siguientes a la notificación de la presente resolución realice lo siguiente:

- Una nueva versión pública del documento "Protocolo de Atención a Incidentes Mayores de Seguridad Informática" en donde se teste la información con carácter de reservada, de conformidad con el artículo 112, fracciones VII y XVI de la Ley General de Transparencia, y la remita de nueva cuenta a este órgano colegiado para su respectivo análisis.

[…]

Por lo expuesto y fundado, se

R E S U E L V E:

[...]

SEGUNDO. Se requiere a la Dirección General de Presupuesto y Contabilidad y a la Dirección General de Tecnologías de la Información en los términos analizados en el apartado II del considerando segundo de esta resolución.
[…]" (*sic*)

[4] CT-CI-A-2-2021.pdf

wwExGMIPGUgDIkUQPBDb9Raz3XelybeA5N2TDQTwNd0=

TERCERO. Notificación de resolución. Por oficios **CT-227-2026** y **CT-228-2026** enviados el dos de junio de dos mil veintiséis, la Secretaría de este Comité notificó a las personas titulares de las Direcciones Generales de Tecnologías de la Información (**DGTI**) y de Presupuesto y Contabilidad (**DGPC**) respectivamente, la resolución transcrita, a efecto de que emitieran los informes requeridos.

CUARTO. Informe de la DGTI. Mediante oficio **UASCJN/DGTI/DAN-126-2026**, de ocho de junio de dos mil veintiséis, el área requerida indicó que a través de la Atenta Nota de Cumplimiento número **UASCJN/DGTI/SGSIC-I-8-2026** da atención al requerimiento formulado, misma nota que anexo al referido oficio, y en la que señaló lo siguiente:

> "[…]
> **Respuesta:**
> **Punto 1 (número de incidentes)**
> Al respecto, me permito informar que, previo a 2011, la Suprema Corte de Justicia de la Nación no contaba con un área especializada de ciberseguridad. A partir de 2011, dichas funciones fueron atendidas por la Dirección de Seguridad Informática, sin que existiera una unidad específica denominada "Ciberseguridad".
> Es en 2021 que se crea la Subdirección de Ciberseguridad y, en 2024, se estableció de manera oficial la Dirección de Ciberseguridad, la cual sustituyó a la Dirección de Seguridad Informática, asumiendo formalmente la atención de las funciones en la materia.
> Por lo anterior, de la búsqueda realizada a los documentos con los que cuenta esta DGTI, se informa que del periodo comprendido de 2007 a 2019 no se localizó información que coincida con lo solicitado por la persona peticionaria.
> No obstante, durante el periodo comprendido entre 2020 al mes de abril del 2026, la Suprema Corte de Justicia de la Nación registró un total de 5,063,343 intentos de ataques cibernéticos. Cabe destacar que ninguno de estos incidentes se concretó, en virtud de que fueron detectados y bloqueados de manera oportuna, conforme al siguiente desglose anual:
>
> | EJERCICIO | TOTAL |
> |---|---|
> | 2020 | 1,225 |
> | 2021 | 1,431 |
> | 2022 | 862,594 |
> | 2023 | 1,149,481 |
> | 2024 | 1,161,974 |
> | 2025 | 1,229,698 |
> | 2026 (abril) | 656,940 |
> | **TOTAL** | **5,063,343** |
>
> **Punto 7, inciso a) (Protocolo de Atención a Incidentes Mayores de Seguridad Informática)**
> Se generó una nueva versión pública del documento "Protocolo de Atención a Incidentes Mayores de Seguridad Informática" en donde se testó la información con carácter de reservada, de conformidad con el artículo 112, fracciones VII y XVI de la Ley General de Transparencia y Acceso a la Información Pública. (Anexo)
> […]" (*sic*)

wwExGMIPGUgDIkUQPBDb9Raz3XelybeA5N2TDQTwNd0=

Asimismo, la **DGTI** adjuntó a su oficio, la copia simple de la nueva versión pública del “Protocolo de Atención a Incidentes Mayores de Seguridad Informática”, en donde se testó información con carácter de reservada, en términos del **artículo 112, fracciones VII** y **XVI** de la Ley General de Transparencia y Acceso a la Información Pública (Ley General de Transparencia).

QUINTO. Informe de la DGPC. Mediante oficio DGPC/06/1385-2026, de veintidós de junio de dos mil veintiséis, el área requerida señaló lo siguiente:

> “[…]
> Hago de su conocimiento que, tras haber realizado un exhaustivo y riguroso segundo análisis a los registros documentales de esta Dirección General, se determinó la inexistencia de información relacionada con el término "ciberseguridad" para el periodo correspondiente a los años 2007 a 2026, no identificando dentro de los capítulos, conceptos o partidas presupuestales ninguna referencia, directa o indirecta, que guarde relación con la materia solicitada.
>
> En estricto apego al marco legal vigente, esta determinación atiende puntualmente lo dispuesto en el artículo 141, segundo párrafo, de la Ley General de Transparencia y Acceso a la Información Pública, el cual rige los criterios normativos ante la ausencia de registros en los archivos de los sujetos obligados, es decir no se cuenta, ni se contaba en el periodo de la solicitud, con atribución o función por parte de esta Dirección General de poseer información con la precisión y detalle de interés de la persona solicitante, por lo que se solicita a ese Comité de Transparencia de la Suprema Corte de justicia de la Nación se de por solventada la omisión señalada en el último párrafo de la página 12 de la resolución CT-VT/A-31-2026 del propio Comité.
>
> […]
>
> Adicionalmente, como parte de las acciones de transparencia proactiva y en estricto cumplimiento con las obligaciones establecidas en los artículos 20, fracción XII, y 65 de la Ley General de Transparencia y Acceso a la Información Pública, se informa que la Suprema Corte de Justicia de la Nación, en su calidad de sujeto obligado, difunde de manera permanente en su Portal Institucional la información financiera y presupuestaria que obra en sus archivos, y que se encuentra disponible para consulta digital el Estado del Ejercicio del Presupuesto (se inserta enlace electrónico), instrumento financiero que permite verificar de forma detallada el presupuesto aprobado y ejercido, mismo que se encuentra estructurado conforme al Clasificador por Objeto del Gasto, herramienta que no contiene ningún capítulo, concepto o partida bajo la denominación de "ciberseguridad"”.
> […]” (*sic*)

SEXTO. Acuerdo de turno. En proveído de nueve de junio de dos mil veintiséis, la Presidencia del Comité de Transparencia de este Alto Tribunal, con fundamento en los artículos 22, 23, fracciones I, II y VIII, 26, fracción V, y 27 del Acuerdo General de Administración 5/2015, ordenó remitir al Titular de la Unidad de Transparencia de la Suprema Corte de Justicia de la Nación (Unidad de Transparencia) en su carácter de Ponente en el asunto de origen, para que conforme a sus atribuciones procediera al

wwExGMIPGUgDIkUQPBDb9Raz3XelybeA5N2TDQTwNd0=

estudio y propuesta de la resolución respectiva, lo que se hizo mediante oficio **CT-243-2026**, de esa misma fecha.

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

PRIMERO. Competencia. El Comité de Transparencia de la Suprema Corte de Justicia de la Nación es competente para para pronunciarse sobre el debido cumplimiento de sus determinaciones, instruir, coordinar y supervisar las acciones y procedimientos para asegurar la eficacia en la gestión de las solicitudes y satisfacer el derecho de acceso a la información, en términos de lo dispuesto en los artículos 6o de la Constitución Política de los Estados Unidos Mexicanos, 4 y 40, fracciones I y II, de la Ley General de Transparencia, así como 23, fracciones I y II y 37 del Acuerdo General de Administración 5/2015.

SEGUNDO. Análisis de cumplimiento. Ahora bien, como se advierte en el apartado de antecedentes, en la resolución del expediente **CT-VT/A-31-2026** se determinó requerir a la **DGPC** a efecto de que realizara una búsqueda exhaustiva y razonable respecto de los registros que dieran cuenta de la baja documental de la información solicitada en los años dos mil siete a dos mil diecinueve; así como para que se pronunciara fundada y motivadamente con relación a la inexistencia planteada respecto del "presupuesto designado al concepto de ciberseguridad" en los ejercicios dos mil veinte a dos mil veintiséis, (**punto 6** inciso **c)** de la solicitud).

Además, a la **DGTI** se le requirió a efecto de que enviara la información relativa al **punto 1**, en cuanto a la información meramente **estadística** con respecto al **número** total de incidentes de ciberseguridad en el periodo solicitado (del uno de enero de dos mil siete al trece de abril de dos mil veintiséis); así como para que del **punto 7**, inciso **a),** proporcionara una nueva versión pública del documento "Protocolo de Atención a Incidentes Mayores de Seguridad Informática", toda vez que se testó información con carácter reservado, en términos del artículo 112, fracciones I y XVI de la Ley General de Transparencia, siendo que este Comité de Transparencia confirmó la reserva con fundamento en las fracciones VII y XVI del citado precepto legal.

En cumplimiento de lo expuesto, la **DGTI**, para el **punto 1,** informó sobre la información estadística que, previo a dos mil once no se contaba con un área

wwExGMIPGUgDIkUQPBDb9Raz3XelybeA5N2TDQTwNd0=

especializada responsable de funciones de ciberseguridad, y a partir de dicho año las funciones fueron atendidas por la Dirección de Seguridad Informática, sin que existiera una unidad específica denominada de ciberseguridad, resultando que en dos mil veintiuno, se creó la Subdirección de Ciberseguridad, y a partir del dos mil veinticuatro, se estableció de manera oficial la Dirección de Ciberseguridad, la cual sustituyó a la Dirección de Seguridad Informática y asumió formalmente la atención de las funciones en la materia.

En ese sentido, indicó que de la búsqueda en los archivos con los que cuenta, se advierte que del dos mil siete al dos mil diecinueve no localizó información que coincida con lo solicitado; no obstante, de dos mil veinte a abril de dos mil veintiséis registró un **total de 5,063,343** intentos de ataques cibernéticos, para lo cual proporcionó el desglose por año.

Además, para el **punto 7,** inciso **a)**, remitió la versión pública del documento “Protocolo de Atención a Incidentes Mayores de Seguridad Informática” testando la información reservada en términos del artículo 112, fracciones VII y XVI de la Ley General de Transparencia.

Por otro lado, la **DGPC** en cumplimiento del requerimiento formulado, respecto del **punto 6**, inciso **c)**, señaló que la inexistencia de información para el periodo de dos mil siete a dos mil veintiséis, se fundamenta en el artículo 141 segundo párrafo de la Ley General de Transparencia, puesto que no cuenta ni contaba con atribución o función de poseer información con la precisión y detalle de interés.

Ante tales circunstancias, se estiman atendidos los requerimientos formulados en el expediente **CT-VT/A-31-2026** a la **DGPC** y a la **DGTI**, y se procede a realizar el estudio correspondiente al tenor de lo que a continuación se expone.

I.- Aspectos atendidos.

Al respecto, de conformidad con el informe de cada una de las instancias, se estima que pueden tenerse por atendidos el **punto 1** sobre el número de incidentes de

wwExGMIPGUgDIkUQPBDb9Raz3XelybeA5N2TDQTwNd0=

dos mil veinte a abril de dos mil veintiséis, y el **punto 7**, inciso **a)**[5], sobre el documento "Protocolo de Atención a Incidentes Mayores de Seguridad Informática" de la solicitud.

Por tanto, la Unidad de Transparencia deberá hacer del conocimiento a la persona solicitante la información referida en este apartado.

II.- Información clasificada.

Al respecto, se precisa que si bien, en la resolución de origen se expresó que la "nueva versión pública del documento "Protocolo de Atención a Incidentes Mayores de Seguridad Informática" en donde se teste la información con carácter de reservada, de conformidad con el artículo 112, fracciones VII y XVI, de la Ley General de Transparencia, y la remita de nueva cuenta a este órgano colegiado para su respectivo análisis" ello fue únicamente para poder cotejar la antigua versión pública con la que se instruyó a entregar. Sin embargo, tanto en la resolución de origen como en los precedentes, se ha clasificado como reservada la información contenida en el Protocolo de Atención a Incidentes Mayores de Seguridad Informática.

En este apartado, es necesario citar lo analizado en la resolución que dio origen a la que ahora se resuelve, es decir, la **CT-VT/A-31-2026**[6], pues en ella, se determinó que la información reservada contenida en el documento "Protocolo de Atención a Incidentes Mayores de Seguridad Informática", debe tener dicho carácter, por actualizar los supuestos establecidos en el artículo 112, fracciones VII y XVI, de la Ley General de Transparencia.

Lo anterior, en virtud de que la divulgación de dicha información revelaría detalles técnicos sobre la seguridad e infraestructura tecnológica de este Máximo Tribunal, así como poner en riesgo el funcionamiento e integridad de los sistemas tecnológicos, y poniendo en riesgo la integridad de los sistemas y la información albergada en ellos, y se obstruiría la prevención de delitos, específicamente el de acceso ilícito a sus equipos y sistemas de informática.

wwExGMIPGUgDIkUQPBDb9Raz3XelybeA5N2TDQTwNd0=

[5] Mismo que será materia de estudio del apartado siguiente.
[6] CT-VT-A-31-2026.pdf

Además, la divulgación de la información solicitada conllevaría un riesgo real, demostrable e identificable, pues se colocaría a la Suprema Corte de Justicia de la Nación en un estado de vulnerabilidad, facilitando una posible intervención de las comunicaciones; así como la usurpación de permisos, suplantación de equipos y de la información almacenada en los servidores; además del robo de información que obran en los archivos digitales, así como el detrimento de las instalaciones tecnológicas.

Para abordar el **análisis de la prueba de daño específica**, se advierte lo siguiente:

a) **Riesgo real, demostrable e identificable.** La difusión de la información plasmada en el Protocolo de Atención a Incidentes Mayores de Seguridad Informática, sobre incidentes de ciberseguridad permitiría a terceros conocer y reconstruir aspectos sensibles de la infraestructura tecnológica de este Alto Tribunal, tales como son vulnerabilidades, capacidades de defensa, patrones de respuesta y sistemas críticos. Ese riesgo es real porque deriva de amenazas existentes en materia de ciberseguridad; demostrable en virtud de que la propia información solicitada contiene elementos técnicos susceptibles de ser utilizados para planear ataques; e identificable puesto que se pueden advertir consecuencias concretas, como accesos ilícitos, extracción de información, afectaciones operativas o reincidencia en vulnerabilidades previamente explotadas.
b) **Riesgo de perjuicio.** El riesgo de perjuicio que supondría la divulgación de la información contenida en el Protocolo Atención a Incidentes Mayores de Seguridad Informática, supera el interés público de su difusión, puesto que se podría comprometer la seguridad institucional y facilitar la comisión de conductas ilícitas previstas en el Código Penal Federal, particularmente aquellas relacionadas con el acceso no autorizado a sistemas informáticos, la obtención o modificación indebida de información y el uso ilícito de datos del Estado. Además, existe la posibilidad de afectar la continuidad operativa de las funciones sustantivas del Alto Tribunal, incluyendo la impartición de justicia, así como poner en riesgo bases de datos, comunicaciones y sistemas estratégicos de la institución.
c) **Limitación adecuada.** Resulta proporcional, ya que representa el medio menos restrictivo para evitar un probable perjuicio a los bienes

wwExGMIPGUgDIkUQPBDb9Raz3XelybeA5N2TDQTwNd0=

jurídicamente protegidos (infraestructura tecnológica). Por lo que, restringir temporalmente su acceso público en la parte que contiene datos técnicos, estratégicos o desagregados relacionados con la seguridad informática institucional, que se plasman en el Protocolo de Atención a Incidentes Mayores de Seguridad Informática. Esta medida se considera jurídicamente válida porque resulta idónea para proteger la infraestructura tecnológica, necesaria al no existir un mecanismo menos restrictivo que garantice el mismo nivel de protección y proporcional, ya que el daño potencial derivado de su divulgación es mayor que el beneficio público de conocerla.

Como se señaló previamente, la reserva de la información se fundamenta en las **fracciones VII y XVI del artículo 112** de la Ley General de Transparencia.

Aunado a lo anterior, se determinó que sobre la información que tiene que ver con el tipo y lugar de origen de los ataques cibernéticos recibidos en este Alto Tribunal de enero a julio de dos mil dieciocho, el plazo de clasificación se encuentra **vigente**[7]; y sobre el resto de información, el plazo procedente para la reserva de la información será por cinco años, a partir de la fecha de dicha resolución, el cual podrá modificarse en caso de que cambien o subsistan las circunstancias que dieron origen a establecerlo.

Con base en la información proporcionada por la **DGTI** se puede tener por atendido el **punto 7**, inciso **a),** de la solicitud y confirmar la reserva de la información contenida en el documento que se analiza en el presente apartado.

III.- Información inexistente.

En este apartado es necesario retomar que para el **punto 1** (número de ataques cibernéticos), la **DGTI** informó que de conformidad con los archivos con los que cuenta, del periodo comprendido entre dos mil siete al dos mil diecinueve no localizó información.

[7] De conformidad con lo establecido en la resolución CT-CUM-A-52-2023.pdf

wwExGMIPGUgDIkUQPBDb9Raz3XelybeA5N2TDQTwNd0=

Además, del **punto 6** inciso **c)**, respecto del periodo de dos mil siete a dos mil veintiséis la **DGPC** informó la inexistencia en virtud de que no cuenta ni contaba con atribución o función de poseer información con la precisión y detalle de interés.

Además, reiteró que la Suprema Corte de Justicia de la Nación, como ejecutora de gasto, registra y reporta la información presupuestaria conforme al Clasificador por Objeto del Gasto, que desagrega los recursos por capítulo, concepto y partida presupuestaria; y dicha estructura constituye el mecanismo reconocido por la normativa presupuestaria y contable para el registro y reporte institucional.

Para analizar la inexistencia anunciada, se recuerda que el derecho de acceso a la información tiene sustento en el artículo 6o, apartado A, de la Constitución Política de los Estados Unidos Mexicanos, cuyo contenido deja claro que, en principio, todo acto de autoridad (todo acto de gobierno) es de interés general y, por ende, es susceptible de ser conocido por todas las personas.

En ese sentido, el acceso a la información pública comprende el derecho fundamental a solicitar, investigar, difundir, buscar y recibir información, que se encuentre integrada en documentos que registren el ejercicio de las facultades, funciones y competencias de los sujetos obligados, lo que obliga a los entes públicos a documentar todo lo relativo a éstas y presume su existencia de acuerdo con los artículos 2, fracción VIII, 3, fracción IX, 4, 8, fracción III, y 16 de la Ley General de Transparencia[8].

wwExGMIPGUgDlkUQPBDb9Raz3XelybeA5N2TDQTwNd0=

[8] "**Artículo 2.** Esta Ley tiene por objeto:
[…]
Fracción VIII. Promover, fomentar y difundir la cultura de la transparencia en el ejercicio de la función pública, el acceso a la información pública, la participación ciudadana y la rendición de cuentas, mediante políticas públicas y mecanismos que garanticen la difusión de información oportuna, verificable, comprensible, actualizada y completa, en los formatos más adecuados y accesibles para el público, tomando en cuenta las condiciones sociales, económicas y culturales de cada región;
[…]"
"**Artículo 3.** Para los efectos de la presente Ley se entiende por:
[…]
IX. Documento: Expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas y, en general, cualquier registro que documente el ejercicio de las facultades, funciones y competencias de los sujetos obligados, sus personas servidoras públicas y demás integrantes, sin importar su fuente o fecha de elaboración, ni el medio en el que se encuentren, ya sea escrito, impreso, sonoro, visual, electrónico, informático u holográfico;
[…]"
"**Artículo 4.** El derecho humano de acceso a la información comprende solicitar, investigar, difundir, buscar y recibir información. Toda la información generada, obtenida, adquirida, transformada o en posesión de los sujetos obligados es pública y accesible a cualquier persona, en los términos y condiciones que se establezcan en la presente Ley, en los tratados internacionales de los que el Estado mexicano sea parte, las leyes de las entidades federativas y en las disposiciones jurídicas aplicables dentro de sus respectivas competencias.
La información podrá ser clasificada como reservada temporalmente por razones de interés público o seguridad nacional conforme a los términos establecidos por esta Ley."
"**Artículo 8.** Las Autoridades garantes deberán regir su funcionamiento de acuerdo a los siguientes principios:
[…]
III. Documentación: Consiste en que los sujetos obligados deberán otorgar acceso a los documentos que se encuentren en sus archivos o que estén obligados a documentar, de acuerdo con sus facultades, competencias o funciones, conforme a las

De esta forma, la existencia de la información (y de su presunción), así como la necesidad de su documentación, se encuentran condicionadas, en todo caso, por la previa vigencia de una disposición legal que, en lo general o en lo particular, delimite el ejercicio de las facultades, competencias o atribuciones por parte de los sujetos obligados respecto de los que se solicite aquella.

Al respecto, se estima que, de conformidad con lo señalado en el artículo 131 de la Ley General de Transparencia, los sujetos obligados están constreñidos a proporcionar la documentación que se encuentre en sus archivos o que estén obligados a documentar, conforme a sus facultades, competencias o funciones, sin necesidad de elaborar documentos *ad hoc*.

Ahora bien, tomando en consideración que la **DGTI** (**punto 1**) y la **DGPC** (**punto 6** inciso **c)**) son competentes para pronunciarse -respectivamente- sobre la materia de lo solicitado, y que tras una nueva búsqueda, la **DGPC** informó, fundando y motivando debidamente, que el documento que concentra el registro de los recursos públicos, concepto y partida presupuestaria es el Clasificador por Objeto del Gasto, aunado a que reiteró que dicho documento no contempla de manera desagregada una partida en específico con el concepto de ciberseguridad.

En ese sentido, tras una búsqueda de información dentro del Clasificador por Objeto del Gasto para los años de interés, no se advirtió una partida presupuestal con concepto designado específicamente a ciberseguridad, razón por la cual, este Comité, estima que actualiza la inexistencia de la información.

Ahora bien, no pasa desapercibido para este Comité que, si bien, la **DGPC** informó sobre ocho bajas documentales, lo cierto es que, dicha circunstancia no incide en el análisis del presente asunto, toda vez que nunca existió un rubro específico de ciberseguridad al cual pudieran corresponder dichas bajas documentales.

wwExGMIPGUgDlkUQPBDb9Raz3XelybeA5N2TDQTwNd0=

características físicas de la información o del lugar donde se encuentre, sin que ello implique la elaboración de documentos ad hoc para atender las solicitudes de información."
"**Artículo 16.** Se presume que la información debe existir cuando se refiere a las facultades, competencias y funciones que los ordenamientos jurídicos aplicables otorgan a los sujetos obligados y se tenga la obligación jurídica de documentarla. En los casos en que ciertas facultades, competencias o funciones no se hayan ejercido, el sujeto obligado deberá motivar la respuesta que lo justifique."

En ese sentido, si las instancias requeridas señalaron que no cuentan con un documento que contenga lo específicamente requerido en el **punto 6**, inciso **c)**, de la solicitud, pues no se advierte la generación del rubro de interés; además, tampoco cuentan con información estadística sobre ataques cibernéticos en el periodo de dos mil siete a dos mil diecinueve requerido en el **punto 1**, se estima que no se está en el supuesto previsto en la fracción I del artículo 140 de la Ley General de Transparencia[9], conforme al cual deban dictarse otras medidas para localizar la información, ya que conforme a la normativa aplicable se trata de las instancias que podrían contar con esa información de conformidad con sus atribuciones, es decir, se ha agotado la búsqueda y no se está en el supuesto de solicitarles que generen la información por devenir de una facultad discrecional que en su momento no se ejerció; por lo que la información resulta inexistente.

Debido a lo vertido anteriormente, este Comité de Transparencia estima válida la inexistencia de la información solicitada en el **punto 1** para el periodo que abarca de dos mil siete a dos mil diecinueve, y en el **punto 6**, inciso **c)**, para el periodo que abraca dos mil siete a dos mil veintiséis.

Por lo expuesto y fundado, se

R E S U E L V E:

PRIMERO. Se tienen por atendidos los requerimientos formulados a la Dirección General de Tecnologías de la Información y a la Dirección General de Presupuesto y Contabilidad.

SEGUNDO. Se tienen por atendidos los puntos analizados en el apartado I del considerando segundo de esta resolución.

TERCERO. Se confirma la clasificación como reservada de la información analizada en el apartado II del considerando segundo de esta resolución.

wwExGMIPGUgDIkUQPBDb9Raz3XelybeA5N2TDQTwNd0=

[9] "**Artículo 140.** Cuando la información no se encuentre en los archivos del sujeto obligado, el Comité de Transparencia:
I. Analizará el caso y tomará las medidas necesarias para localizar la información;
[…]"

CUARTO. Se confirma la inexistencia de la información analizada en el apartado III del considerando segundo de esta resolución.

QUINTO. Se solicita a la Unidad de Transparencia que realice lo determinado en esta resolución.

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

Así, por unanimidad de votos, lo resolvió el Comité de Transparencia de la Suprema Corte de Justicia de la Nación y firman la **Maestra Camelia Gaspar Martínez**, Directora General de Asuntos Jurídicos y Presidenta del Comité; el **Maestro Abraham Montes Magaña**, Titular de la Unidad de Transparencia de la Suprema Corte de Justicia de la Nación; y, el **Doctor Gustavo Miguel Meixueiro Nájera**, Director General del Centro de Documentación y Análisis, Archivos y Compilación de Leyes; integrantes del Comité, ante la Secretaria del Comité, quien autoriza y da fe.

MAESTRA CAMELIA GASPAR MARTÍNEZ
PRESIDENTA DEL COMITÉ

MAESTRO ABRAHAM MONTES MAGAÑA
INTEGRANTE DEL COMITÉ

DOCTOR MIGUEL MEIXUEIRO NÁJERA
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.

wwExGMIPGUgDIkUQPBDb9Raz3XelybeA5N2TDQTwNd0=