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

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 **veintiocho de mayo 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, la persona solicitante 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
>
> Para cada año, solicito el desglose por:
> - Tipo de incidente:
> - Acceso no autorizado
> - *Ransomware*
> - *Malware*
> - Filtración de información
> - Ataques a sistemas críticos
> - Otros (especificar)
> - Número de incidentes por tipo.
>
> 2. Para cada incidente (o en versión agregada por año, en caso de limitaciones), solicito:
> - Fecha o periodo en que ocurrió
> - Tipo de sistema afectado (bases de datos, servidores, sistemas críticos, etc.)
> - Tipo de información comprometida:

DQBpBoIml/5qTimIMr8Pp97iP+1XkIyINUtJwyDaIQM=

- Datos personales
- Datos sensibles
- Información estratégica o de seguridad
- Información administrativa

- Número estimado de registros o personas afectadas (en su caso)
- Entidad o área interna afectada

3. Solicito, desagregado por año:
- Número de eventos de filtración o vulneración de datos personales
- Tipo de datos comprometidos (nombre, CURP, RFC, datos financieros, biométricos, etc.)
- Número de personas afectadas

Asimismo, indicar:
- Si se notificó a las personas afectadas
- Si se notificó al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales
- Fecha de dichas notificaciones

4. Solicito se informe, por año, si los incidentes identificados fueron:
- De origen interno
- De origen externo
- Mixto o indeterminado

En su caso, indicar si se identificaron:
- Grupos responsables
- Tipología de actores (ciberdelincuencia, hacktivismo, etc.)

5. Para cada año, solicito:
- Acciones de contención, mitigación y remediación implementadas
- Cambios en políticas, sistemas o infraestructura derivados de los incidentes
- Acciones de mejora en ciberseguridad

6. Solicito, desagregado por año:
- Existencia de áreas o unidades responsables de ciberseguridad
- Número de personal asignado a dichas funciones
- Presupuesto destinado a ciberseguridad

7. Solicito:
- Protocolos de atención a incidentes de ciberseguridad
- Manuales, lineamientos o políticas internas aplicables
- Fundamento normativo aplicable

8. Solicito, por año, información sobre:
- Colaboración con otras dependencias federales
- Participación en estrategias nacionales de ciberseguridad
- Mecanismos de coordinación ante incidentes

Solicito que la información sea entregada en formato electrónico y, de ser posible, en datos abiertos (Excel o CSV).

En caso de que la información solicitada se encuentre clasificada, solicito se entregue versión pública, testando únicamente los datos estrictamente confidenciales o reservados. En caso de inexistencia parcial o total, solicito se funde y motive conforme a la normatividad aplicable.” [sic]

SEGUNDO. Acuerdo de apertura de expediente. Por acuerdo de quince de abril de dos mil veintiséis, el Subdirector General de Acceso a la Información adscrito a Unidad de Transparencia de la Suprema Corte de Justicia de la Nación (Unidad de Transparencia), una vez analizados la naturaleza y contenido de la solicitud, la determinó procedente y ordenó abrir el expediente electrónico **UT/A/0406/2026**.

DQBpBoIml/5qTimIMr8Pp97iP+1XkIyINUtJwyDaIQM=

TERCERO. Requerimiento de información. Una vez formado el expediente, por oficios número **SCJN/UT/SGAI-1060-2026**, y **SCJN/UT/SGAI-1316-2026**, enviados el dieciséis de abril, y doce de mayo del presente año, el Subdirector General de Acceso a la Información, por instrucciones del Titular de la Unidad de Transparencia, requirió a la persona Titular de la **Dirección General de Tecnologías de la Información** de la Unidad de Administración de la Suprema Corte de Justicia de la Nación (**DGTI**); así como a la de la **Dirección General de Presupuesto y Contabilidad** de la Unidad de Administración de la Suprema Corte de Justicia de la Nación (**DGPC**), en el orden mencionado, para que en el ámbito de sus respectivas competencias se pronunciaran sobre la información solicitada.

CUARTO. Informe de la DGTI. Mediante oficio número **UASCJN/DGTI/SGPNA-DA-96-2026**, de veintitrés de abril de dos mil veintiséis, la referida instancia proporcionó respuesta al requerimiento formulado, señalando que adjuntaba la Atenta nota **UASCJN/DGTI/SGSIC-I-4-2026** signada por personal adscrito a la Subdirección General de Seguridad Informática y Ciberseguridad, misma que se detalla en los términos siguientes:

> "[…]
>
> *[Se transcriben los puntos 1 a 5 de la solicitud]*
>
> **Respuesta:**
>
> Al respecto, se informa que la información **solicitada se considera reservada**, de conformidad con el artículo 112, fracciones VII y XVI de la Ley General de Transparencia y Acceso a la Información Pública (se inserta vínculo electrónico para consulta y en adelante Ley General), mediante la siguiente prueba de daño:
>
> Se acredita que existe un riesgo real, demostrable e identificable relativa a incidentes de ciberseguridad, vulneraciones de datos personales, tipología de ataques, sistemas afectados, origen de los incidentes, así como acciones de contención, mitigación y remediación implementadas, permitiría inferir, con un alto grado de precisión, las capacidades operativas, arquitectura de seguridad, patrones de respuesta y posibles vulnerabilidades de la infraestructura tecnológica de la Suprema Corte de Justicia de la Nación.
>
> En ese sentido, la divulgación de dicha información generaría, entre otros, los siguientes efectos:
>
> - Permitir la identificación de patrones de comportamiento de incidentes y frecuencia de ataques, facilitando la planeación de ataques dirigidos;
> - Revelar indirectamente la arquitectura de defensa, protocolos de seguridad y capacidades de respuesta institucional;
> - Exponer vectores de ataque previamente explotados, lo que incrementa la probabilidad de reincidencia o explotación de vulnerabilidades similares;
> - Permitir inferir la capacidad de detección, contención y reacción institucional, debilitando la eficacia de los mecanismos de seguridad;

DQBpBoImI/5qTimIMr8Pp97iP+1XkIyINUtJwyDaIQM=

- Facilitar la identificación de sistemas críticos, bases de datos o infraestructura sensible, susceptibles de ser comprometidos;
- Incrementar el riesgo de accesos ilícitos, suplantación de identidad, intervención de comunicaciones y extracción de información;
- Generar condiciones propicias para la modificación, destrucción o pérdida de información institucional;
- Comprometer la continuidad operativa de las funciones sustantivas del Alto Tribunal, particularmente en la impartición de justicia.

La divulgación de la información solicitada incrementa de manera sustancial la probabilidad de que terceros realicen conductas tipificadas en el Código Penal Federal, particularmente en materia de acceso ilícito a sistemas y equipos de informática.

En términos de los artículos 211 Bis 1, 211 Bis 2 y 211 Bis 7 del citado ordenamiento, se sanciona:

- El acceso no autorizado a sistemas informáticos protegidos;
- La obtención, copia, modificación o destrucción de información;
- El uso indebido de información obtenida de sistemas del Estado.

En este contexto, la información solicitada constituye un insumo que, de hacerse público, facilitaría la comisión de dichas conductas, al proporcionar elementos técnicos y estratégicos que permiten reducir los niveles de incertidumbre de un posible atacante.

La clasificación de la información como reservada cumple con el principio de proporcionalidad, en virtud de que:

- La restricción a la publicidad es idónea, ya que evita la exposición de información estratégica en materia de ciberseguridad;
- Es necesaria, dado que no existe una medida menos restrictiva que permita proteger la seguridad de los sistemas institucionales sin comprometer su funcionamiento;
- Es proporcional en sentido estricto, toda vez que el daño potencial derivado de su divulgación es mayor que el beneficio de hacerla pública en los términos solicitados.

Asimismo, se advierte que:

- La entrega de la información en forma desagregada permitiría reconstruir el estado real de la seguridad informática institucional;
- La reserva constituye el medio menos lesivo para proteger los bienes jurídicos involucrados, sin impedir el acceso a información general o normativa.

Si bien el principio de máxima publicidad rige el acceso a la información, en el presente caso el riesgo de perjuicio que supondría la divulgación de la información solicitada supera el interés público de su conocimiento en forma desagregada y técnica, debido a que su difusión comprometería la seguridad institucional y facilitaría la comisión de ilícitos.

Por tanto, resulta procedente la clasificación como información reservada de los elementos solicitados en los numerales 1, 2, 3, 4 y 5, en sus componentes técnicos, operativos y estratégicos.

Ahora bien, en cuanto al periodo de **reserva**, el artículo 104 de la Ley General, establece que **la información clasificada** podrá permanecer con tal carácter, hasta por un periodo de cinco años, en el caso concreto, considerando que el bien jurídico tutelado es la prevención de un delito, **se considera que el periodo de reserva debe ser de 5 años**.

Por último, todo lo anteriormente expuesto se refuerza con lo resuelto por el Comité de Transparencia a través de los expedientes de Clasificación de Información CT-CI-A-2-2021 y de Cumplimiento CT-CUM/A-52-2023 derivado del expediente CT-CUM/A-36/2018 (se inserta vínculo electrónico para consulta).

[Se transcribe el punto 6 de la solicitud]

DQBpBoImI/5qTimIMr8Pp97iP+1XkIyINUtJwyDaIQM=

Respuesta:

Al respecto, se informa que para los años previos a 2011, la Suprema Corte de Justicia de la Nación no contaba con un área especializada responsable de funciones de ciberseguridad, a partir del año 2011, dichas funciones fueron atendidas por la Dirección de Seguridad Informática, sin que existiera una unidad específica denominada de ciberseguridad, a partir del año 2021 se crea la Subdirección de Ciberseguridad, y a partir del año 2024, 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

El Número de personal asignado a dichas funciones entre los años del 2021 a 2023 fueron de 4 personas de la Subdirección de Ciberseguridad, y de entre los años del 2024 a 2026, han sido de 5 personas de la Dirección de Ciberseguridad.

Asimismo, respecto al presupuesto designado a ciberseguridad, se informa que el área encargada de coordinar las actividades de planeación, programación, presupuestación, así como de dar seguimiento al ejercicio del presupuesto de egresos asignado a la Suprema Corte y la ejecución de los programas anuales de necesidades autorizados es la **Dirección General de Presupuesto y Contabilidad**, por lo que, **se estima conveniente turnarle esta solicitud de transparencia para su pronunciamiento**.

[Se transcribe el punto 7 de la solicitud viñeta 1 “Protocolos de atención a incidentes de ciberseguridad” (sic)]

Respuesta:

Al respecto, se cuenta con la versión púbica del “Protocolo de Atención a Incidentes Mayores de Seguridad Informática” con vigencia a partir de noviembre de 2022 (Anexo I)

[Se transcribe el punto 7 de la solicitud viñeta 2 “Manuales, lineamientos o políticas internas aplicables” (sic)]

Respuesta:

Al respecto, se cuenta con el Manual del Sistema de Gestión de Seguridad de la Información (Seguridad Informática) (Anexo II); Políticas de Seguridad Informática. Administradores de Sistemas Informáticos (Anexo III); Políticas de Seguridad Informática. Personas Usuarias (Anexo IV).

[Se transcribe el punto 7 de la solicitud viñeta 3 “Fundamento normativo aplicable” (sic)]

Respuesta:

Al respecto, se cuenta con el Acuerdo General de Administración Número VIII/2022 Uso y aprovechamiento de los bienes y servicios de tecnologías de la información y comunicaciones, así como de la seguridad informática; y el Manual de Organización Específico DGTI (se insertan vínculos electrónicos para consulta).

[Se transcribe el punto 8 de la solicitud]

Respuesta:

De la búsqueda realizada a los documentos con los que cuenta esta DGTI se informa que no se localizó información que coincida con lo solicitado por el peticionario; en este sentido, resulta aplicable lo señalado en el segundo párrafo del artículo 141 de la Ley General de Transparencia y Acceso a la Información Pública (se inserta vínculo electrónico para consulta), en lo relativo a que, en aquellos casos en que no se advierta obligación o competencia alguna de los sujetos obligados para contar con la información, derivado del análisis a las disposiciones jurídicas aplicables a la materia de la solicitud, además no se tengan elementos de convicción que permitan suponer que esta debe obrar en sus archivos, o bien, se cuente con atribuciones, pero no se ha generado la información no será necesario que el Comité de Transparencia emita una resolución que confirme la inexistencia de la misma.

DQBpBoImI/5qTimIMr8Pp97iP+1XkIyINUtJwyDaIQM=

> Asimismo, en cumplimiento al principio de máxima publicidad se informa que no se cuenta formalmente con colaboración con otras dependencias federales, ni participación institucional en estrategias nacionales de ciberseguridad o mecanismos de coordinación de incidentes con otras dependencias federales; sin embargo, se precisa que el "Protocolo de Atención a Incidentes Mayores de Seguridad Informática", con vigencia a partir de noviembre de 2022 a la fecha, tomó como modelo de referencia operativo el Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos (PNHGIC), emitido por la Guardia Nacional, por lo que contempla notificar al CERT-MX de la Guardia Nacional de México exclusivamente respecto de incidentes mayores de ciberseguridad que, en su caso, pudieran llegar a materializarse.
>
> […]" (sic)

Asimismo, la **DGTI** adjuntó a su respuesta la copia simple de los documentos siguientes:

A. Versión pública del "Protocolo de Atención a Incidentes Mayores de Seguridad Informática".

B. Manual del Sistema de Gestión de Seguridad de la Información (Seguridad Informática).

C. Políticas de Seguridad Informática Administradores de Sistemas Informáticos.

D. Políticas de Seguridad Informática Personas Usuarias.

QUINTO. Ampliación del plazo. Mediante oficio número **SCJN/UT/SGAI-1281-2026**, enviado por correo electrónico el seis de mayo de dos mil veintiséis, la Unidad de Transparencia solicitó la ampliación del plazo ordinario de respuesta, la cual fue autorizada por este Comité de Transparencia en su Novena Sesión Ordinaria de dos mil veintiséis, y así lo informó la Secretaría del Comité con el oficio número **CT-152-2026** de siete de mayo de dos mil veintiséis, lo que se notificó a la persona solicitante a través de la Plataforma Nacional de Transparencia en la misma fecha.

SEXTO. Informe de la DGPC. Mediante oficio número **DGPC/05/1109-2026**, de trece de mayo de dos mil veintiséis, la referida instancia proporcionó respuesta al requerimiento formulado, señalando que adjunta la Nota de cumplimiento número **DGPC/SGP-041-2026**, signada por el Subdirector General de Presupuesto, misma que se detalla en los términos siguientes:

DQBpBoIml/5qTimIMr8Pp97iP+1XkIyINUtJwyDaIQM=

> "[…]
>
> III. Atención puntual a la solicitud.
>
> Se informa 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 (se inserta vínculo electrónico para su consulta), que desagrega los recursos por capítulo, concepto y partida presupuestaria. Esta estructura constituye el mecanismo reconocido por la normativa presupuestaria y contable para el registro y reporte institucional.
>
> Por lo anterior, le comento que respecto al punto donde se solicita el presupuesto designado al concepto de ciberseguridad señalado en el numeral 6, le informo que para los ejercicios de 2020 a 2026, no se cuenta con la información, atendiendo en todo momento lo dispuesto en el artículo 131 de la Ley General de Transparencia y Acceso a la Información Pública.
>
> Asimismo, se hace de su conocimiento que los expedientes presupuestales y contables relativos a los ejercicios fiscales 2019 y anteriores, concluyeron con su ciclo archivístico, por tal motivo fue procedente su baja documental, de conformidad con los artículos 7 fracción V, 33 y 34 del Acuerdo General de Administración número XI/2021, emitido por el Presidente de la Suprema Corte de Justicia de la Nación el cinco de octubre de 2021, resultando aplicable lo señalado en el artículo 141, segundo párrafo, de la Ley General de Transparencia y Acceso a la información Pública.
>
> Finalmente, en lo correspondiente a los demás puntos del numeral 6, le comento que la Dirección General de Presupuesto y Contabilidad no cuenta con atribuciones para atender la misma, conforme a lo establecido en el artículo 31 del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación (publicado en el Diario Oficial de la Federación el día 6 de mayo de 2022).
>
> […]" (sic)

SÉPTIMO. Remisión del expediente electrónico a la Secretaría del Comité de Transparencia de la Suprema Corte de Justicia de la Nación. Por oficio electrónico número **SCJN/UT/SGAI-1313-2026**, de catorce de mayo de dos mil veintiséis, el Subdirector General de Acceso a la Información remitió el expediente electrónico a la cuenta electrónica institucional de la Secretaría del Comité de Transparencia de la Suprema Corte de Justicia de la Nación, a efecto de que le asignara el turno correspondiente y se elaborara el proyecto de resolución respectivo.

OCTAVO. Acuerdo de radicación y turno. Mediante proveído de catorce de mayo de dos mil veintiséis, la Presidencia del Comité de Transparencia de este Alto Tribunal, con fundamento en los artículos 40, fracción II, de la LGTAIP, 23, fracción II, y 27 del Acuerdo General de Administración 05/2015, ordenó integrar el expediente **CT-VT/A-31-2026** y, conforme al turno correspondiente, remitirlo a la persona Titular de la Unidad de Transparencia, a fin de que presentara la propuesta de resolución correspondiente.

DQBpBoIml/5qTimIMr8Pp97iP+1XkIyINUtJwyDaIQM=

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 conocer y resolver el presente asunto, 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 y Acceso a la Información Pública (Ley General de Transparencia), así como 23, fracciones I y II, del Acuerdo General de Administración 5/2015.

SEGUNDO. Análisis. Como se relató en el capítulo de antecedentes, se advierte que la persona solicitante requirió, conocer en formato electrónico, y de ser posible, en datos abiertos, del **primero de enero de dos mil siete al trece de abril de dos mil veintiséis**, información relacionada con incidentes, filtraciones de información, capacidades institucionales y acciones implementadas en torno a la materia de ciberseguridad; en específico lo siguiente:

1. El número total de incidentes de ciberseguridad registrados por la dependencia, desagregado por año y por:

a) Tipo de incidente: Acceso no autorizado, *Ransomware*, *Malware*, Filtración de información, Ataques a sistemas críticos, otros (especificar).

b) Número de incidentes por tipo.

2. Para cada incidente:

a) Fecha o periodo en que ocurrió.

b) Tipo de sistema afectado (bases de datos, servidores, sistemas críticos, etcétera).

c) Tipo de información comprometida: Datos personales, Datos sensibles, Información estratégica o de seguridad, Información administrativa.

d) Número estimado de registros o personas afectadas (en su caso).

e) Entidad o área interna afectada.

3. Desagregado por año:

a) Número de eventos de filtración o vulneración de datos personales.

b) Tipo de datos comprometidos [nombre, Clave Única de Registro de Población (CURP), Registro Federal de Contribuyentes (RFC), datos financieros, biométricos, etcétera].

c) Número de personas afectadas.

DQBpBoImI/5qTimIMr8Pp97iP+1XkIyINUtJwyDaIQM=

Asimismo, indicar:

d) Si se notificó a las personas afectadas.

e) Si se notificó al extinto Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

f) Fecha de dichas notificaciones.

4. Se informe por año, si los incidentes fueron:

a) De origen interno.

b) De origen externo.

c) Mixto o indeterminado

En su caso, indicar si se identificaron:

d) Grupos responsables.

e) Tipología de actores (ciberdelincuencia, hacktivismo, etcétera).

5. Para cada año, conocer:

a) Acciones de contención, mitigación y remediación implementadas.

b) Cambios en políticas, sistemas o infraestructura derivados de los incidentes.

c) Acciones de mejora en ciberseguridad.

6. Desagregado por año, conocer:

a) Existencia de áreas o unidades responsables de ciberseguridad.

b) Número de personal asignado a dichas funciones.

c) Presupuesto destinado a ciberseguridad.

7. Conocer:

a) Protocolos de atención a incidentes de ciberseguridad.

b) Manuales, lineamientos o políticas internas aplicables.

c) Fundamento normativo aplicable.

8. Conocer, por año:

a) Colaboración con otras dependencias federales.

b) Participación en estrategias nacionales de ciberseguridad.

c) Mecanismos de coordinación ante incidentes.

En ese sentido, se requirió a la persona titular de la **DGTI**, para que se pronunciara en el ámbito de su competencia; por lo que, la referida instancia, indicó que la información requerida en los **puntos 1 a 5** de la solicitud es **reservada** de conformidad con el **artículo 112, fracciones VII y XVI** de la Ley General de Transparencia, para lo cual proporcionó la prueba de daño que consideró conveniente, en los términos que se plasman en el antecedente Cuarto de la presente resolución.

DQBpBoImI/5qTimIMr8Pp97iP+1XkIyINUtJwyDaIQM=

Respecto del **punto 6** inciso **a)**, indicó que para los años previos a dos mil once, no se contaba con un área 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, a partir de 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.

Asimismo, sobre el **punto 6** inciso **b)**, señaló que el número de personal asignado a dichas funciones entre los años dos mil veintiuno a dos mil veintitrés fueron de cuatro personas de la Subdirección de Ciberseguridad, y de dos mil veinticuatro a dos mil veintiséis han sido de cinco personas de la Dirección de Ciberseguridad.

Respecto del **punto 7** inciso **a),** informó que cuenta con la versión pública del "Protocolo de Atención a Incidentes Mayores de Seguridad Informática" con vigencia a partir de noviembre de dos mil veintidós, mismo que anexó. Sobre el inciso **b)** del referido **punto 7**, señaló que cuenta con el Manual del Sistema de Gestión de Seguridad de la Información (Seguridad Informática), así como las "Políticas de Seguridad Informática. Administradores de Sistemas Informáticos" y las "Políticas de Seguridad Informática. Personas Usuarias" mismos que puso a disposición. Por último, respecto del inciso **c)** del **punto 7**, indicó que cuenta con el "Acuerdo General de Administración Número VIII/2022" por el que se regula el uso y aprovechamiento de los bienes y servicios de tecnologías de la información y comunicaciones, así como de la seguridad informática; y el "Manual de Organización Específico DGTI" para lo cual proporcionó los vínculos electrónicos para su consulta.

Sobre el **punto 8** de la solicitud, indicó que no localizó información que coincida con lo solicitado, sin que se advierta obligación o competencia alguna para poseer la información, sin embargo, en atención al principio de máxima publicidad, indicó que no se cuenta formalmente con colaboración con otras dependencias federales, ni participación institucional en estrategias nacionales de ciberseguridad o mecanismos de coordinación de incidentes con otras dependencias federales; sin embargo, señaló que el "Protocolo de Atención a Incidentes Mayores de Seguridad Informática" tomó

DQBpBoIml/5qTimIMr8Pp97iP+1XkIyINUtJwyDaIQM=

como modelo de referencia operativo el “Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos” (PNHGIC) emitido por la Guardia Nacional, por lo que contempla notificar al CERT-MX de la Guardia Nacional de México exclusivamente respecto de incidentes mayores de ciberseguridad que, en su caso, pudieran llegar a materializarse.

Por otro lado, la **DGPC** en su informe señaló que con respecto al **punto 6** inciso **c)** de la solicitud, 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.

I.- Aspectos atendidos

Al respecto, de conformidad con el informe de cada una de las instancias, se estima que pueden tenerse por atendidos los **puntos 6** incisos **a)** y **b)**, **7 inciso a)** y **8**[1] de la solicitud.

Ahora bien, se debe resaltar que el análisis de la versión pública del “Protocolo de Atención a Incidentes Mayores de Seguridad Informática” proporcionada por la **DGTI** para dar atención al **punto 7** inciso **a)** será materia de un apartado subsecuente.

Por otro lado, no pasa desapercibido para este Comité que, en atención al inciso **b)** del **punto 7**, la **DGTI** proporcionó el Manual del Sistema de Gestión de Seguridad de la Información (Seguridad Informática), al respecto, se advierte que el referido documento fue puesto a disposición en versión íntegra; sin embargo, , se identificó que

DQBpBoIml/5qTimIMr8Pp97iP+1XkIyINUtJwyDaIQM=

[1] Pues si bien es cierto que la instancia requerida informó que no localizó expresión documental que atendiera lo solicitado, que no cuenta formalmente con colaboración con otras dependencias federales, ni participación institucional en estrategias nacionales de ciberseguridad o mecanismos de coordinación de incidentes, también lo es que en atención al principio de máxima publicidad indicó que el “Protocolo de Atención a Incidentes Mayores de Seguridad Informática” tomo como modelo de referencia operativo el “PNHGIC” emitido por la Guardia Nacional, por lo que se contempla notificar al CERT-MX de la Guardia Nacional en caso de incidentes mayores de ciberseguridad que pudieran suscitarse.

en atención a un folio diverso[2] al que nos ocupa, dicho Manual ya había sido entregado en **versión pública**, por contener información clasificada como reservada consistente en los "Resultados de la evaluación de riesgos de seguridad informática" a los sistemas críticos de la Suprema Corte de Justicia de la Nación, pues el resguardo de dicha información implica llevar a cabo la prevención del delito de acceso ilícito a sistemas y equipos de informática.

Por tanto, la Unidad de Transparencia deberá poner a disposición de la persona solicitante la versión pública del Manual del Sistema de Gestión de Seguridad de la Información (Seguridad Informática) analizada en dos mil veintitrés; así como hacer de su conocimiento el resto de la información referida en este apartado.

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[3] 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

[2] CT-CI-A-35-2023.pdf
[3] **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**].

DQBpBoIml/5qTimIMr8Pp97iP+1XkIyINUtJwyDaIQM=

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[4], 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 **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)**

[4] "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;"

DQBpBoImI/5qTimIMr8Pp97iP+1XkIyINUtJwyDaIQM=

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[5], 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,

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

DQBpBoImI/5qTimIMr8Pp97iP+1XkIyINUtJwyDaIQM=

fracciones VII y XVI de la Ley General de Transparencia, y la remita de nueva cuenta a este órgano colegiado para su respectivo análisis.

III.- Información clasificada como reservada

En este apartado, se debe recordar que la **DGTI**, indicó que la información requerida en los **puntos 1** a **5** de la solicitud es **reservada** de conformidad con el **artículo 112, fracciones VII y XVI** de la Ley General de Transparencia.

Al respecto, el Pleno del Alto Tribunal ha interpretado, en diversas ocasiones, que el derecho de acceso a la información no puede caracterizarse como 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[6].

En atención a la disposición constitucional referida, 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.

Resulta necesario señalar que el **artículo 112, fracciones VII y XVI** de la Ley General de Transparencia establece lo siguiente:

> "**Artículo 112.** Como información reservada podrá clasificarse aquella cuya publicación:
>
> […]

[6] ***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)*

DQBpBoImI/5qTimIMr8Pp97iP+1XkIyINUtJwyDaIQM=

> **VII.** Pueda causar daño u obstruya la prevención o persecución de los delitos, altere el proceso de investigación de las carpetas de investigación, afecte o vulnere la conducción o los derechos del debido proceso en tanto no hayan quedado firmes o afecte la administración de justicia o la seguridad de una persona denunciante, querellante o testigo, así como sus familias, en los términos de las disposiciones jurídicas aplicables;
>
> […]
>
> **XVI.** Ponga en riesgo el funcionamiento o integridad de los sistemas tecnológicos, energéticos, espaciales, satelitales, de telecomunicaciones o de defensa desarrollados, adquiridos u operados por el Gobierno Federal de forma directa o indirecta, así como instalaciones, infraestructuras, proyectos, planes o servicios de protección estratégicos, prioritarios o de defensa, y
>
> […]" (*sic*)

Ahora bien, no pasa desapercibido que las razones expuestas para motivar la reserva de la información de los **puntos 1 incisos a)** y **b) a 5** de la solicitud es que, de revelarse podría facilitar la frecuencia de ataques al permitir la identificación de patrones de comportamiento de incidentes, así como revelar la arquitectura de defensa, protocolos de seguridad y capacidad de respuesta; afectando vectores de ataque previamente explotados, interfiriendo la capacidad de detección, contención y reacción institucional, así como identificarse los sistemas críticos, bases de datos o infraestructura sensible, susceptibles de ser comprometidos, aumentando el riesgo de accesos ilícitos, suplantación de identidad, intervención de comunicaciones y extracción de información, entre otros posibles escenarios de vulnerabilidad.

En ese sentido, la información relacionada con incidentes de ciberseguridad (**puntos 1 incisos a)** y **b) a 5** de la solicitud, a excepción de lo referido en el apartado anterior) en el periodo comprendido entre el uno de enero de dos mil siete al trece de abril de dos mil veintiséis, constituye información **reservada**, en tanto que la instancia vinculada refiere que son 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 múltiples servidores de esta Suprema Corte de Justicia de la Nación.

Además, la **DGTI** al realizar la prueba de daño argumentó que de divulgarse la información solicitada en dichos puntos, incrementaría de manera sustancial la probabilidad de que terceros realicen conductas tipificadas en el Código Penal Federal en los artículos 211 Bis 1, 211 Bis 2 y 211 Bis 7[7], particularmente en materia de acceso

[7] "**Artículo 211 bis 1.-** Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

DQBpBoIml/5qTimIMr8Pp97iP+1XkIyINUtJwyDaIQM=

ilícito a sistemas y equipos de informática; es decir, la información solicitada resulta un insumo que, de divulgarse facilitaría la comisión de dichas conductas, al proporcionar elementos técnicos y estratégicos que permiten reducir niveles de incertidumbre de un posible atacante.

Aunado a lo anterior, la reserva de la información es proporcional en virtud de que se evitaría la exposición de información estratégica en materia de ciberseguridad, toda vez que el daño potencial derivado de su publicidad es mayor que el beneficio de hacerla pública en los términos solicitados, además de que la información con la desagregación solicitada permite reconstruir el estado real de la seguridad informática institucional, por lo que la reserva constituye el medio menos lesivo para proteger los bienes jurídicos tutelados, sin que ello impida el acceso a información general o normativa.

A mayor abundamiento, se debe retomar lo sustentado por este Comité de Transparencia al resolver el expediente **CT-CUM/A-52-2023**[8], en el sentido de que el daño que se podría producir con la divulgación de la información relativa al tipo y lugar de origen de los ataques cibernéticos recibidos por la Suprema Corte de Justicia de la Nación “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”, así como el expediente **CT-CUM-R/A-2-2019**[9], en el cual se expuso que “La divulgación de la información solicitada conllevaría un riesgo real, demostrable e identificable, en tanto que colocaría a la Suprema Corte de Justicia de la Nación en un estado de

DQBpBoIml/5qTimIMr8Pp97iP+1XkIyINUtJwyDaIQM=

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.
Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.
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.
A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.
Las sanciones anteriores se duplicarán cuando la conducta obstruya, entorpezca, obstaculice, limite o imposibilite la procuración o impartición de justicia, o recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes.
[…]
Artículo 211 bis 7.- Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.”
[8] CT-CUM-A-52-2023.pdf
[9] CT-CUM-R-A-2-2019.pdf

vulnerabilidad, facilitando una posible intervención de las comunicaciones; usurpación de permisos; suplantación de equipos y de la información almacenada en los servidores; robo de información que obran en los archivos digitales, así como el detrimento de las instalaciones tecnológicas.”

Bajo esa línea argumentativa, la reserva de la información solicitada representa el medio menos restrictivo del derecho de acceso a la información, al considerarse la trascendencia de proteger, desde un esquema global, la infraestructura informática de este Alto Tribunal en tanto que se podrían involucrar negativamente aspectos de seguridad pública, y con ello, facilitar posibles ataques cibernéticos.

Así, abordando el **análisis de la prueba de daño específica**, se advierte que se actualizan las razones objetivas de un riesgo real, demostrable e identificable, así como el riesgo de perjuicio que supera el interés púbico, y la limitación adecuada, tal y como se detalla a continuación:

a) **Riesgo real, demostrable e identificable.** La difusión de la información técnica y desagregada 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, supera el interés público de su difusión, porque 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

DQBpBoIml/5qTimIMr8Pp97iP+1XkIyINUtJwyDaIQM=

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 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. 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, bajo los argumentos expuestos respecto de que la divulgación 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.

Al respecto, es importante destacar que el informe lo emite el área técnica que, conforme a las atribuciones que le confiere el artículo 36 del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación, es responsable de los servicios y sistemas informáticos sobre los que versa la solicitud que da origen a este asunto y, tomando como base lo resuelto por este Comité en diversas resoluciones[10], en las que se analizó información similar, se arriba a la conclusión sobre que los **puntos 1 a 5** de la solicitud, efectivamente **constituye información reservada** en los términos analizados en este apartado (a excepción de lo analizado en el apartado anterior).

[10] CT-CUM-R/A-2-2019, CT VT/A-11-2025, CT-CUM/A-6-2025 y CT-CUM-A-52-2023.

DQBpBoIml/5qTimIMr8Pp97iP+1XkIyINUtJwyDaIQM=

Plazo de reserva. Con base en lo expuesto, y con fundamento en el artículo 104 de la Ley General de Transparencia, se determina lo siguiente:

Para los puntos relacionados 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**[11].

Ahora bien, respecto del resto de información, el plazo procedente para la reserva de la información será por cinco años, a partir de la fecha de la presente resolución, el cual podrá modificarse en caso de que cambien o subsistan las circunstancias que dieron origen a establecerlo.

Por lo expuesto y fundado, se

R E S U E L V E:

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

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.

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

CUARTO. Se instruye a la Unidad de Transparencia a realizar lo determinado en esta resolución.

Notifíquese a la persona solicitante, a las instancias requeridas 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**

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

DQBpBoImI/5qTimIMr8Pp97iP+1XkIyINUtJwyDaIQM=

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.

DQBpBoIml/5qTimIMr8Pp97iP+1XkIyINUtJwyDaIQM=