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

CLASIFICACIÓN DE INFORMACIÓN
CT-CI/A-35-2023

INSTANCIAS VINCULADAS:

DIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN

UNIDAD GENERAL DE TRANSPARENCIA Y SISTEMATIZACIÓN DE LA INFORMACIÓN JUDICIAL

Ciudad de México. Resolución del Comité de Transparencia de la Suprema Corte de Justicia de la Nación, correspondiente al **veintitrés de agosto de dos mil veintitrés.**

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

I. Solicitud de información. El siete de julio de dos mil veintitrés se recibió a través de la Plataforma Nacional de Transparencia la solicitud tramitada bajo el folio **330030523001697**, en la que se requirió:

> *"1. Me pueden indicar si la institución dispone de un Sistema de Gestión de Seguridad de la Información?*
>
> *2. En caso afirmativo me pueden compartir la versión pública del documento.*
>
> *3. Qué estándar para la seguridad de la información se tiene implementado en la institución?*
>
> *4. De favor si me pueden compartir los documentos de seguridad de sus sistemas de datos personales."* [sic].

II. Acuerdo de admisión. Por acuerdo de siete de julio de dos mil veintitrés, el Subdirector General de la Unidad General de Transparencia y Sistematización de la Información Judicial (Unidad General de Transparencia), una vez analizados la naturaleza y contenido de la solicitud, la determinó procedente y ordenó abrir el expediente electrónico **UT-A/0487/2023.**

En el mismo proveído, por lo que hace a lo requerido en el **punto 4** de la solicitud, al tratarse de información vinculada con las atribuciones conferidas a la Unidad General de Transparencia, se instruyó emitir un informe en el que se determinara su existencia y, en su caso, su clasificación.

III. Requerimiento de información. Por oficio electrónico UGTSIJ/TAIPDP-

bF/wOflJfPkwcqbjfJjJUtZqEtFR938T4t0GuGPu0e4=

3829-2023 de diez de julio de dos mil veintitrés, la Titular de la Unidad General de Transparencia requirió a la Dirección General de Tecnologías de la Información para que se pronunciara sobre la existencia de la información solicitada en los **puntos 1, 2 y 3**, su correspondiente clasificación, modalidad disponible y, en su caso, el costo de su reproducción.

IV. Ampliación del plazo global del procedimiento. En sesión ordinaria de nueve de agosto de dos mil veintitrés el Comité de Transparencia autorizó ampliar el plazo ordinario de resolución de la presente solicitud de información.

V. Presentación de informe. Por oficio electrónico DGTI/339/2023 de nueve de agosto de dos mil veintitrés, el Titular de la Dirección General de Tecnologías de la Información manifestó lo siguiente:

> *"[…] Al respecto, se adjunta Atenta Nota de Cumplimiento con número DGTI/DSI/14/2023, signada por Mtro. Omar Salinas García, Director de Seguridad Informática y el Mtro. Ramón Caballero Ledesma, Subdirector de Cumplimiento de Seguridad Informática, mediante la cual se proporciona la información solicitada. […]"*

"[…] **Atención al oficio UGTSIJ/TAIPDP-3829-2023 referente a la solicitud de información con folio PNT 330030523001697 y folio interno UT-A/0487/2023**"

Fecha de elaboración:	09/08/2023
Nota de cumplimiento DGTI/DSI/14/2023	

ATENTA NOTA AL DIRECTOR GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN

[…] Al respecto, se informa que la Dirección General de Tecnologías de la Información (DGTI), es competente para atender esta solicitud, acorde a lo previsto en el artículo 36 del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación (ROMA), la que cuenta con la Dirección de Seguridad Informática (DSI) adscrita a dicha Dirección General, cuyas funciones están relacionadas con la solicitud que se atiende.

Por lo que se refiere a la parte de la solicitud que requiere: ***1. Me pueden indicar si la institución dispone de un Sistema de Gestión de Seguridad de la Información.? (sic)***

Respuesta:

Se informa al solicitante que este Alto Tribunal sí cuenta con un Sistema de Gestión de Seguridad de la Información (SGSI) que está en proceso de actualización y mejora conforme a la normatividad que entró en vigor a finales del año 2022, consistente en el Acuerdo General de Administración (AGA

bF/wOflJfPkwcqbjfJjjUtZqEtFR938T4t0GuGPu0e4=

VIII/2022) del Comité de Gobierno y Administración de la Suprema Corte de Justicia de la Nación, por el que se regulan el uso y aprovechamiento de los bienes y servicios de tecnologías de la información y comunicaciones, así como de la seguridad informática[1].

Por lo que se refiere a la parte de la solicitud que señala: ***En caso afirmativo me pueden compartir la versión pública del documento. (sic)***

Respuesta:

Se proporciona la versión pública del documento, el cual se adjunta mediante el archivo en formato accesible 'MAN-SGSI-01P Manual SGSI_v.2.1_Información.pdf'

Cabe señalar que el documento mencionado se adjunta en versión pública, por contener información clasificada como reservada, consistente en: 'Resultados de evaluación de riesgos de seguridad informática' a los sistemas críticos de la Suprema Corte de Justicia de la Nación (SCJN), con fundamento en los artículos 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP) y 113, fracción Vll de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP). Para efecto de lo anterior, se realiza la siguiente prueba de daño:

- *Existe un riesgo real, demostrable e identificable de perjuicio significativo al interés público, toda vez que la difusión de los 'Resultados de evaluación de riesgos de seguridad informática' sobre los sistemas críticos de la SCJN, implicaría colocar en un estado de vulnerabilidad a la Suprema Corte de Justicia de la Nación, ya que al entregar dicha información se comprometería la seguridad informática de los sistemas y equipos de este Alto Tribunal, porque se pondría en riesgo la seguridad operativa de la infraestructura tecnológica que permite la operación de las diversas áreas del Alto Tribunal.*
- *Se supera el interés público general de que se difunda la información, ya que el resguardo de la información requerida en la solicitud implica llevar a cabo la prevención del delito de acceso ilícito a sistemas y equipos de informática tipificado en el Código Penal Federal, lo cual cobra importancia si se considera que dicha conducta implica conocer, copiar, modificar, destruir o provocar la pérdida de información contenida en sistemas o equipos de informática, por lo que revelar los 'Resultados de evaluación de riesgos de seguridad informática' no sólo comprometería la información que obra en los archivos digitales del sujeto obligado, sino que menoscabaría la seguridad y certeza de los ciudadanos que acuden a este Alto Tribunal para otorgar certeza respecto de la impartición de justicia y control constitucional. En este sentido, la divulgación de la información:*
  - ✓ *Permitiría el acceso ilícito a sus sistemas y equipos informáticos, intentando la suplantación de los mismos;*
  - ✓ *Potenciaría la posibilidad de vulnerar la seguridad de su infraestructura tecnológica;*
  - ✓ *Establecería con un alto grado de precisión la información técnica referente a los protocolos de seguridad y las características de la*

[1] Disponible para consulta en: https://www.scjn.gob.mx/conoce-la-corte/marconormativo/public/api/download?fileName=AGA%20VIII-2022%20DGTI-CGA%20VF(1).pdf

bF/wOflJfPkwcqbjfJjJUtZqEtFR938T4t0GuGPu0e4=

infraestructura instalada;

- ✓ *Pondría en un estado vulnerable a la institución, facilitando la intervención de las comunicaciones y permitiendo usurpar permisos requeridos en la red para obtener información;*
- ✓ *Daría a conocer puntos de vulnerabilidad para la seguridad de la infraestructura de cómputo;*
- ✓ *Vulneraría sus sistemas informáticos, así como la información contenida en éstos;*
- ✓ *Atentaría en contra de su infraestructura tecnológica, afectando el ejercicio de sus labores sustantivas; y*
- ✓ *Modificaría, destruiría o provocaría pérdida de información contenida en sus sistemas.*

- *Clasificar la información como reservada se adecua al principio de proporcionalidad, en tanto que se justifica negar su divulgación se motiva en pretender evitar o prevenir la comisión del delito de acceso ilícito a sus equipos y sistemas de informática. Ello, aunado a que la clasificación constituye el medio menos lesivo para la adecuada protección del bien jurídico tutelado, como es la seguridad pública general.*

Derivado de todo lo anterior, cabe preciar que el Código Penal Federal dispone lo siguiente:

'TITULO NOVENO

Revelación de secretos y acceso ilícito a sistemas y equipos de informática

(…)

CAPÍTULO II

Acceso ilícito a sistemas y equipos de informática

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.

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 de 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 de 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.

bF/wOflJfPkwcqbjfJjJUtZqEtFR938T4t0GuGPu0e4=

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.' (sic)

De los preceptos antes citados, se advierte que comete el delito de acceso ilícito a sistemas y equipo 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, mencionan que, a quien 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 de multa.

De igual forma, la entrega de 'Resultados de evaluación de riesgos de seguridad informática', podría ocasionar lo siguiente:

- ✓ *La usurpación de sus permisos de acceso a sus sistemas crítico;*
- ✓ *La afectación de la disponibilidad de sus sistemas críticos, y*
- ✓ *El robo de la información que obra en sus sistemas críticos.*

Todo lo anteriormente expuesto, se refuerza con lo resuelto por el Comité de Transparencia de la Suprema Corte de Justicia de la Nación, a través de la resolución del expediente CT-CUM-R/A-2-2019, derivado del CT-CI/A-27-2018, que indica lo siguiente:

'…En cumplimiento de lo determinado por el Instituto Nacional de Transparencia, en el sentido de que este Comité debe dictar una resolución en la que confirme la reserva temporal de la información solicitada con fundamento en la fracción VII del artículo 110 de la Ley Federal de Transparencia y Acceso a la Información Pública, se procede a emitir el pronunciamiento correspondiente, por lo que se transcribe dicho artículo:

'Artículo 110. Conforme a lo dispuesto por el artículo 113 de la Ley General, como información reservada podrá clasificarse aquella cuya publicación:

(…)

VII. Obstruya la prevención o persecución de los delitos;

Sobre el alcance de dicho precepto, en la resolución emitida en el recurso de revisión que se cumplimenta, se señala que 'como información reservada podrá clasificarse aquella cuya 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 precisa 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, agregando: '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'

Enseguida se hace alusión al Código Penal Federal señalando que '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

bF/wOflJfPkwcqbjfJjjUtZqEtFR938T4t0GuGPu0e4=

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'

…

En virtud de lo anterior, en la resolución se argumenta que '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 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', conforme al artículo 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, en específico, la obstrucción a la prevención de delitos.

Así como lo referido en la resolución CT-CI/A-7-2020, de la cual se resalta lo siguiente:

'…Ahora bien, para sustentar la clasificación de reserva que hace la Dirección General de Tecnologías de la Información, se cita el artículo 110, fracción VII, de la Ley Federal de Transparencia, manifestando que su divulgación:

- *Permitiría el acceso ilícito a los sistemas y equipos, ejerciendo la suplantación de estos.*
- *Potenciaría la posibilidad de vulnerar la infraestructura tecnológica.*
- *Establecería con alto grado de precisión la información técnica sobre los protocolos de seguridad y las características de la infraestructura instalada.*
- *Se pondría en estado vulnerable a la Suprema Corte de Justicia de la Nación, porque se facilitaría la intervención de las comunicaciones, permitiendo usurpar los permisos requeridos en la red para obtener información.*
- *Daría a conocer puntos de vulnerabilidad para la seguridad de la infraestructura de cómputo.*
- *Vulneraría los sistemas informáticos y la información contenida en éstos.*
- *Atentaría contra la infraestructura tecnológica, afectando el ejercicio de las labores sustantivas.*
- *Modificaría, destruiría o provocaría pérdida de información contenida en los sistemas informáticos.*

La clasificación como reservada de dicha información, como se señaló, se sustenta en el artículo 110, fracción VII, de la Ley Federal de Transparencia, en virtud de que al poner en riesgo cuestiones de seguridad y conectividad de los sistemas informáticos y bases de datos de la Suprema Corte de Justicia de la Nación se obstruiría la prevención de delitos, específicamente, delito de acceso ilícito a sus equipos y sistemas de informática.

…

De conformidad con lo expuesto, atendiendo a los argumentos señalados por el Instituto Nacional de Transparencia en el recurso de revisión RRA 10276/18 y que fueron retomados en la resolución CT-CUM-R/A-2-2019, este Comité de Transparencia confirma la clasificación de reserva de la información relativa a las políticas de vulnerabilidad implementadas para la prevención y solución de amenazas conforme a cada elemento para la protección de los sistemas de la Suprema Corte de Justicia de la Nación (punto 3 de la solicitud), con fundamento en los artículos 113, fracción VII, de la Ley General de Transparencia y 110, fracción VII, de la Ley Federal de la materia dado que, como se mencionó, considerando que la Dirección General de Tecnologías

bF/wOflJfPkwcqbjfJjjUtZqEtFR938T4t0GuGPu0e4=

de la Información es el área técnica para pronunciarse sobre la naturaleza de la información solicitada y dicha área señaló que al entregar esos datos se podría comprometer la seguridad informática de los sistemas y equipos de este Alto Tribunal, porque se pondría en riesgo la seguridad operativa de la infraestructura tecnológica que permite la operación de las diversas áreas del Alto Tribunal.

Así, conforme a la argumentación sostenida en la resolución del Instituto Nacional de Transparencia la reserva de dicha información permite prevenir la comisión del delito de acceso ilícito a sistemas y equipos de Informática tipificados en el Código Penal Federal, pues al dar a conocer la información solicitada, no sólo se 'comprometería la información que obra en los archivos digitales del sujeto obligado, sino que menoscabaría la seguridad y certeza de los ciudadanos que acuden a éste para otorgar certeza respecto de la impartición de justicia y control constitucional'.

Por lo tanto, se confirma se confirma la reserva de la información materia de este apartado, con fundamento en los artículos 110, fracción VII, de la Ley Federal de Transparencia y 113, fracción VII, de la Ley General de Transparencia. (sic)'.

Ahora bien, en cuanto al periodo de reserva, el artículo 99 de la LFTAIP, 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, 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.

Finalmente, por lo que se refiere a la parte que solicita: ***3.- Que estándar para la seguridad de la información se tiene implementado en la institución.***

Respuesta:

Se informa que el estándar de referencia con el que actualmente se implementa el SGSI es el ISO/IEC 27001:2013. Cabe precisar que la norma antes mencionada es una norma internacional que permite el aseguramiento, la confidencialidad, integridad y disponibilidad de los datos y de la información, así como de los sistemas que la procesan. […]

VI. Presentación de informe interno. Mediante acuerdo de catorce de agosto de dos mil veintitrés, la **Unidad General de Transparencia**, informó lo siguiente:

"[…] El presente pronunciamiento se circunscribirá a la información requerida bajo el último de los numerales comprendidos en dicha solicitud.

En este orden de ideas, hágase del conocimiento del solicitante que en estos momentos, esta Unidad General se encuentra actualizando el contenido del Documento de Seguridad (en lo sucesivo ***Documento de Seguridad 2023****).*

Cabe destacar que el ***Documento de Seguridad 2023*** *contiene información estratégica para el diseño y la ejecución de la implementación de medidas de seguridad necesarias para proteger los datos personales que posee este Alto Tribunal, en particular, el reporte de riesgo que ilustra precisamente el nivel de éste de cada uno de los tratamientos que se encuentran bajo resguardo de cada una de las área u órganos (Anexo 1 y Anexo 2), así como los resultados derivados del análisis de brecha (Anexo 3 y Anexo 4). Dicha información, en esencia, refleja las prácticas de seguridad de la información*

bF/wOflJfPkwcqbjfJjJUtZqEtFR938T4t0GuGPu0e4=

con las que cuenta en ese momento el sujeto obligado y las que deberían de tenerse con base en las mejores prácticas.

En ese sentido, se estima necesario reservar parcialmente el Documento de Seguridad respecto de sus cuatro anexos que contienen los resultados obtenidos en los análisis de riesgo identificado [sic] *y el análisis de brecha, pues su divulgación implica un riesgo real, demostrable e identificable en perjuicio al interés público, que actualiza las fracciones I y VII del artículo 113 de la Ley General de Transparencia y Acceso a la Información Pública en relación con las fracciones I y VII del artículo 110 de la Ley Federal de Transparencia y Acceso a la Información Pública, en particular, por comprometer la seguridad pública y la obstrucción a la prevención de delitos.*

Cabe señalar que el propio Comité de Transparencia confirmó la clasificación parcial del primer Documento de Seguridad aprobado en el año de 2019, en el expediente CT-I/A-11-2022 [sic]*, cuyos argumentos se sostienen en el presente asunto pues, a consideración de esta Unidad General, se actualizan al tratarse de la actualización del propio Documento de Seguridad materia de la reserva aludida.*

La sola divulgación de los niveles de riesgo identificados por cada tratamiento y el análisis de brecha reflejarían el grado de vulnerabilidad de la institución en materia de seguridad de la información, así como las capacidades institucionales de reacción para mitigar los riesgos.

Por ejemplo, la divulgación de la información que se protege vulneraría la seguridad informática de este Alto Tribunal, pues se genera la expectativa razonable de que ocurra un ataque intrusivo que pudiera inhabilitar el uso y funcionamiento de las medidas de seguridad implementadas, lo cual afectaría el desempeño de la función jurisdiccional y de las áreas administrativas, además de que se pondría en peligro la confidencialidad e integridad de los datos personales que posee la institución.

Por tanto, a consideración de esta Unidad General se actualizan las causales de reserva previstas en las fracciones I y VII del artículo 113 de la Ley General, así como sus correlativas del artículo 110 de la Ley Federal:

> *‘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;*
>
> *(…)*
>
> *VII. Obstruya la prevención o persecución de los delitos;’*
>
> *(…)*
>
> *‘Artículo 110. Conforme a lo dispuesto por el artículo 113 de la Ley General, 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;*
>
> *(…)*
>
> *VII. Obstruya la prevención o persecución de los delitos;’*

bF/wOflJfPkwcqbjfJjJUtZqEtFR938T4t0GuGPu0e4=

(…)

Sobre el alcance de la fracción I de los preceptos transcritos, de acuerdo con los 'Lineamientos generales en materia de clasificación y desclasificación de la información', artículo Décimo octavo[2]*, se considera un riesgo a la seguridad pública la divulgación de aquella información que pueda poner en riesgo las funciones a cargo de la Federación tendientes a preservar y resguardar la vida, la salud, la integridad y el ejercicio de los derechos de las personas.*

Luego, sobre el alcance del artículo 110, fracción VII de la Ley Federal de Transparencia, cuyo contenido es idéntico al que hace referencia la Ley General de la materia en el artículo 113, fracción VII, se tiene presente lo resuelto por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales en el recurso de revisión RRA 10276/18, cumplimentada por este Comité en la resolución CT-CUM-R/A-2-2019, en la que se señaló que 'como información reservada podrá clasificarse aquella cuya 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'*** *(página 98, vuelta de la resolución del recurso de revisión RRA 10276/18).*

Además, 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, agregando: '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 se considera prevención del delito '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', considerando 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'.*

Por tanto, debe considerarse acertado que se clasifique como reservada temporalmente la información señalada, en términos de la fracciones I y VII, del artículo 113 de la Ley General de Transparencia y 110, fracciones I y VII, de la Ley Federal de la materia, ya que de no reservarse, se vulnerarían las medidas de protección al divulgarse la información clasificada, generando la

[2] *'**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.*
Se pone en peligro el orden público cuando la difusión de la información pueda entorpecer los sistemas de coordinación interinstitucional en materia de seguridad pública, menoscabar o dificultar las estrategias contra la evasión de reos; o menoscabar o limitar la capacidad de las autoridades encaminadas a disuadir o prevenir disturbios sociales.
Asimismo, podrá considerarse como reservada aquella que revele datos que pudieran ser aprovechados para conocer la capacidad de reacción de las instituciones encargadas de la seguridad pública, sus planes, estrategias, tecnología, información, sistemas de comunicaciones.

bF/wOflJfPkwcqbjfJjJUtZqEtFR938T4t0GuGPu0e4=

expectativa razonable de que ocurra un ataque intrusivo a las bases de datos personales en posesión de este Alto Tribunal, pudiendo, incluso, afectar el desempeño de la función jurisdiccional y de las áreas administrativas de este Alto Tribunal.

*Esto es así, en tanto que el análisis de riesgo que se desarrolla en el **Documento de Seguridad - 2023**, identifica los diversos factores de riesgo a que están expuestos los tratamientos de datos personales y calcula el riesgo latente de cada uno de ellos; y, en el análisis de brecha, identifica la distancia que existe entre las medidas recomendadas y las medidas implementadas por cada uno de los tratamientos reportados, es decir, ubica las medidas de seguridad que hacen falta implementar para el resguardo de los datos personales y cuyos resultados dan sustento a las políticas y mecanismos institucionales en materia de protección de datos personales.*

Con la reserva se busca proteger la información y las bases de datos personales, evitando exponerlas a un ataque que pudiera conseguir vulnerarlas u obtenerlas para beneficiarse de ellas, lo que pondría en riesgo la privacidad de las personas titulares y podría ser causa de responsabilidad de la Suprema Corte de Justicia de la Nación, en términos de los deberes y las causas de incumplimiento de las obligaciones, especialmente de las vulneraciones previstas en los artículos 38 y 41 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Por lo tanto, su divulgación representa un riesgo real, demostrable e identificable de perjuicio significativo a la seguridad de la información y al derecho de protección de datos personales de los titulares de dicha información, ante lo cual no puede prevalecer el interés particular del peticionario, sino un interés mayor de proteger esa información.

*A mayor abundamiento, se estima que se actualiza el supuesto de reserva previsto en la fracción I del artículo 113 de la Ley General de Transparencia, pues divulgar 'los niveles de riesgo identificados' y 'el análisis de brecha' contenidos en los anexos del **Documento de Seguridad - 2023**, podría vulnerar el derecho a la protección de datos personales en posesión de la Suprema Corte de Justicia de la Nación, ya que se conocería el nivel y las medidas de protección implementadas por este Alto Tribunal para cada uno de los tratamientos de datos personales que se encuentran bajo su resguardo, así como el grado de vulnerabilidad de la institución en materia de seguridad de la información y las capacidades institucionales de reacción para enfrentar el mal uso de los datos personales que se encuentran bajo resguardo de este Alto Tribunal, lo que actualiza el supuesto de reserva contenido en la fracción VII del artículo 113 de la citada Ley General de Transparencia.*

PRUEBA DE DAÑO

Aunado a lo expuesto, al estar en presencia de una limitación del derecho de acceso a la información pública, corresponde examinar la implementación de la reserva en el caso particular. Para ello, debe analizarse si la limitación (i) persigue una finalidad constitucionalmente imperiosa, (ii) si es idónea para satisfacer en alguna medida su propósito constitucional, (iii) si existen medidas alternativas igualmente idóneas para lograr dicho fin, pero que sean menos lesivas para el derecho fundamental, y (iv) si el grado de realización

bF/wOflJfPkwcqbjfJjJUtZqEtFR938T4t0GuGPu0e4=

del fin perseguido es mayor al grado de afectación provocado al derecho de acceso a la información por la reserva.

Como se estableció previamente, la reserva de la información busca proteger la seguridad de la información y al derecho de protección de datos personales de los titulares de dicha información, ante lo cual no puede prevalecer el interés particular del peticionario, sino un interés mayor de proteger esa información, por lo que la medida cuenta con una finalidad válida, ya que busca tutelar otros valores de rango constitucional.

La reserva es idónea, porque con ello se evita la vulneración o indebido tratamiento que pudieran recibir los datos personales que tiene en resguardo este Alto Tribunal, comprometiendo con ello la seguridad de la información y el derecho a la protección de sus datos personales de los titulares, pues la difusión de dicha información puede poner en peligro la integridad y el ejercicio de los derechos de las personas, de ahí que la reserva es apta y contribuye al fin perseguido.

Por lo que hace a la necesidad de la reserva, debe señalarse que la reserva se refiere al 'análisis de riesgo' y al 'análisis de brecha' contenidos en los anexos del ***Documento de Seguridad - 2023****. Se estima que la divulgación de esa información sí puede vulnerar el derecho a la protección de datos personales en posesión de este Alto Tribunal, pues como ya se señalaba, podría poner en riesgo la estrategia de seguridad implementadas para proteger los datos personales que se encuentran bajo su resguardo, al divulgarse los niveles de riesgo identificados en los tratamientos de datos personales y con el análisis de la brecha se daría a conocer el grado de vulnerabilidad de esta institución en materia de seguridad de protección de datos personales, lo que, se reitera, representa un riesgo real para la seguridad pública y de las personas.*

Además, no existe un medio alternativo que pudiera garantizar el derecho de acceso a la información respecto de la información reservada, sin que implique en alguna medida un riesgo para los valores protegidos por la misma. No obstante, la entrega de la versión pública del ***Documento de Seguridad – 2023*** *sin sus anexos se erige como el medio menos restrictivo que consigue balancear el derecho de acceso a la información y los valores protegidos por la reserva.*

Por último, se estima que la reserva es proporcional a la acotación del acceso a la información pública, pues se busca proteger las bases de datos personales que obran en resguardo de este Alto Tribunal, evitando exponerlas a un ataque que pudiera conseguir vulnerarlas u obtenerlas para beneficiarse de ellas, lo que podría poner en riesgo la privacidad de las personas titulares, ante lo cual debe rendirse el interés público de acceso a esa información en particular.

Por las anteriores consideraciones, lo procedente es confirmar la reserva al actualizarse el supuesto de las fracciones I y VII del artículo 113 de la Ley General de Transparencia y artículo 110, fracciones I y VII de la Ley Federal de la materia, quedando reservada la siguiente información antes analizada:

- Anexo 1. Análisis de Riesgo 2022
- Anexo 2. Análisis de Riesgo 2022

bF/wOflJfPkwcqbjfJjlJtZqEtFR938T4t0GuGPu0e4=

- Anexo 3. Comparativo de brecha
- Anexo 4: Análisis de brecha 2022

Fundamento

Artículos 113, fracciones I y VII, primer párrafo, 131 y 137 de la Ley General de Transparencia y Acceso a la Información Pública; 110, fracciones I y VII, 133 y 140 de la Ley Federal de Transparencia y Acceso a la Información Pública; 16, párrafo quinto, del Acuerdo General de Administración 05/2015, del tres de noviembre de dos mil quince, del Presidente de la Suprema Corte de Justicia de la Nación, por el que se expiden los Lineamientos Temporales para regular el procedimiento administrativo interno de Acceso a la Información Pública, así como el funcionamiento y atribuciones del Comité de Transparencia de la Suprema Corte de Justicia de la Nación. […]"

VII. Remisión del expediente electrónico a la Secretaría del Comité de Transparencia de la Suprema Corte de Justicia de la Nación. Mediante oficio electrónico **UGTSIJ/TAIPDP-4382-2023** de dieciséis de agosto de dos mil veintitrés, la Titular de la Unidad General de Transparencia remitió el expediente electrónico a la cuenta electrónica institucional de la Secretaria de este Comité, a efecto de que le asignara el turno correspondiente y se elaborara el proyecto de resolución respectivo.

VIII. Acuerdo de turno. Mediante acuerdo de dieciséis de agosto de dos mil veintitrés, el Presidente del Comité de Transparencia ordenó su remisión al **Titular de la Unidad General de Investigación de Responsabilidades Administrativas 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 la 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 N D O:

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

bF/wOflJfPkwcqbjfJjJUtZqEtFR938T4t0GuGPu0e4=

II. Análisis de la solicitud. Del análisis integral de la solicitud, se advierte que se requiere saber:

1. Si esta institución dispone de un Sistema de Gestión de Seguridad de la Información
2. En caso afirmativo, solicita la versión pública del documento respectivo
3. Qué estándar se tiene implementado para la seguridad de la información
4. Los documentos de seguridad de los sistemas de datos personales de este Alto Tribunal

Para atender lo solicitado en los **puntos 1, 2 y 3**, se requirió a la Dirección General de Tecnologías de la Información (**DGTI**), y respecto del **punto 4**, la Unidad General de Transparencia proporcionó información, a partir de lo cual se hará el análisis correspondiente a continuación.

1. Información que se tiene por atendida.

En relación con la información solicitada en el **punto 1,** la DGTI informó que en este Alto Tribunal **sí se cuenta con un Sistema de Gestión de Seguridad de la Información (SGSI)**, el cual está en proceso de actualización y mejora conforme a la normativa que entró en vigor a finales del año 2022, consistente en el Acuerdo General de Administración (AGA VIII/2022)[3], del Comité de Gobierno y Administración de la Suprema Corte de Justicia de la Nación, por el que se regulan el uso y aprovechamiento de los bienes y servicios de tecnologías de la información y comunicaciones, así como de la seguridad informática de la Suprema Corte de Justicia de la Nación, con lo que se atiende este aspecto de la solicitud.

En el **punto 3,** la persona solicitante pide conocer qué estándar se tiene implementado para la seguridad de la información, respecto de lo cual la DGTI informó que el estándar de referencia con el que actualmente se implementa el SGSI es el ISO/IEC 27001:2013 y, al respecto, precisó se trata de una norma internacional que permite el aseguramiento, la confidencialidad, integridad y disponibilidad de los datos y de la información, así como de los sistemas que la procesan, con lo que se tiene por atendido este punto.

[3] Disponible para consulta en: AGA VIII/2022 (SCJN)

bF/wOfIJfPkwcqbjfJjJUtZqEtFR938T4t0GuGPu0e4=

En mérito de lo anterior, se instruye a la Unidad General de Transparencia que haga del conocimiento de la persona solicitante la información proporcionada por la DGTI.

2. Información reservada

En el **punto 2** de la solicitud, se pide la versión pública del documento relativo al Sistema de Gestión de Seguridad de la Información y en el **punto 4**, los documentos de seguridad de los sistemas de datos personales de este Alto Tribunal.

En relación con la información solicitada en el **punto 2,** la DGTI pone a disposición de la persona solicitante la versión pública del Manual del Sistema de Gestión de Seguridad de la Información de este Alto Tribunal, por contener información clasificada como reservada, consistente en los "Resultados de 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, lo cual fundamenta en los artículos 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública (Ley Federal de Transparencia) y 113, fracción Vll, de la Ley General de Transparencia.

Por lo que hace a la información que se pide en el **punto 4,** la Unidad General de Transparencia informó que el **Documento de seguridad 2023,** contiene información estratégica para el diseño y la ejecución de la implementación de medidas de seguridad necesarias para proteger los datos personales que posee este Alto Tribunal.

En particular, el reporte de riesgo que ilustra precisamente el nivel de éste de cada uno de los tratamientos que se encuentran bajo resguardo de cada una de las áreas u órganos (Anexo 1 y Anexo 2), así como los resultados derivados del análisis de brecha (Anexo 3 y Anexo 4), que en esencia reflejan las prácticas de seguridad de la información con las que cuenta en ese momento el sujeto obligado y, las que deberían de tenerse con base en las mejores prácticas.

En ese sentido, clasificó parcialmente el referido documento de seguridad respecto de sus cuatro anexos que contienen los resultados obtenidos en los

bF/wOflJfPkwcqbjfJjlUtZqEtFR938T4t0GuGPu0e4=

análisis de riesgo identificado y el análisis de brecha, lo que sustenta en las fracciones I y VII del artículo 113 de la Ley General de Transparencia en relación con las fracciones I y VII del artículo 110 de la Ley Federal de Transparencia, en particular, por comprometer la seguridad pública u obstruir la prevención de delitos.

Ahora bien, para confirmar o no la clasificación realizada por las instancias vinculadas respecto a esa información se tiene presente que, en nuestro sistema constitucional, el derecho de acceso a la información encuentra cimiento 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.

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 de contenido absoluto, sino que su ejercicio está acotado en función de ciertas causas e intereses relevantes, así como frente al necesario tránsito de las vías adecuadas para ello[4].

En atención a la disposición constitucional antes referida, se obtiene que la información bajo resguardo de los sujetos obligados del Estado es pública, pero encuentra como excepción aquélla que sea temporalmente reservada o confidencial en los términos establecidos por el legislador, cuando de su propagación pueda derivarse perjuicio por causa de interés público y seguridad nacional.

bF/wOfIJfPkwcqbjfJjJUtZqEtFR938T4t0GuGPu0e4=

[4] Véase la tesis P. LX/2000 del Pleno de la Suprema Corte de Justicia de la Nación, publicada en el Semanario Judicial de la Federación y su Gaceta, Novena Época, Abril de 2000, Tomo XI, página 74, registro digital 2006870, cuyo rubro y texto es del tenor literal siguiente: “**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.”

En desarrollo de ese extremo de excepcionalidad, el artículo 113 de la Ley General de Transparencia establece un catálogo genérico de supuestos bajo los cuales debe reservarse la información, lo cual procederá cuando su otorgamiento o publicación pueda: **1)** comprometer la seguridad nacional, la seguridad pública o la defensa nacional y cuente con un propósito genuino y un efecto demostrable; **2)** menoscabar la conducción de las negociaciones y relaciones internacionales; **3)** afectar la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país; pueda poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país, pueda comprometer la seguridad en la provisión de moneda nacional al país, o pueda incrementar el costo de operaciones financieras que realicen los sujetos obligados del sector público federal; **4)** poner en riesgo la vida, seguridad o salud de una persona física; **5)** obstruir las actividades de verificación, inspección y auditoría relativas al cumplimiento de las leyes o afecte la recaudación de contribuciones; **6)** obstruir la prevención o persecución de delitos; **7)** afectar los procesos deliberativos de los servidores públicos, hasta en tanto no sea adoptada la decisión definitiva; **8)** obstruir los procedimientos para fincar responsabilidad a los servidores públicos, en tanto no se haya dictado la resolución administrativa; **9)** afectar los derechos del debido proceso; **10)** vulnerar la conducción de los expedientes judiciales o de los procedimientos administrativos seguidos en forma de juicio, en tanto no hayan causado estado; **11)** se encuentre dentro de una investigación ministerial, y **12)** por disposición expresa de otra ley.

Junto a la identificación de esos supuestos y con el ánimo de proyectar a cabalidad el principio constitucional que les da sentido, la Ley General de Transparencia en sus artículos 103, 104, 108 y 114[5], exige que en la definición sobre

bF/wOflJfPkwcqbjfJjlUtZqEtFR938T4t0GuGPu0e4=

[5] **Artículo 103**. En los casos en que se niegue el acceso a la información, por actualizarse alguno de los supuestos de clasificación, el Comité de Transparencia deberá confirmar, modificar o revocar la decisión.
Para motivar la clasificación de la información y la ampliación del plazo de reserva, se deberán señalar las razones, motivos o circunstancias especiales que llevaron al sujeto obligado a concluir que el caso particular se ajusta al supuesto previsto por la norma legal invocada como fundamento. Además, el sujeto obligado deberá, en todo momento, **aplicar una prueba de daño**.
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.
Artículo 108. Los sujetos obligados no podrán emitir acuerdos de carácter general ni particular que clasifiquen Documentos o información como reservada. La clasificación podrá establecerse de manera parcial o total de acuerdo al contenido de la información del Documento y deberá estar acorde con la actualización de los

su configuración, además de la realización de un examen casuístico y de justificación fundado y motivado, se desarrolle la aplicación de una prueba de daño; entendida como el estándar que implica ponderar la divulgación de la información frente a la actualización de un daño.

En este sentido, a efecto de determinar si es correcto o no el pronunciamiento de las áreas vinculadas se tiene presente que en términos del artículo 100, último párrafo, de la Ley General de Transparencia[6], en relación con el diverso 17, párrafo primero, del Acuerdo General de Administración 5/2015[7], las personas titulares de las instancias que tienen bajo resguardo la información requerida son responsables de determinar su disponibilidad y clasificarla conforme a la normativa aplicable.

En el caso concreto de la información solicitada en el punto 2, 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[8] del Reglamento Orgánico en Materia de Administración de la Suprema

---

supuestos definidos en el presente Título como información clasificada.
En ningún caso se podrán clasificar Documentos antes de que se genere la información.
La clasificación de información reservada se realizará conforme a **un análisis caso por caso, mediante la aplicación de la prueba de daño**.
Artículo 114. Las causales de reserva previstas en el artículo anterior se deberán fundar y motivar, a través de la **aplicación de la prueba de daño** a la que se hace referencia en el presente Título.

[6] "**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."

[7] "**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.
[…]"

[8] "**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

bF/wOflJfPkwcqbjfJjlJUtZqEtFR938T4t0GuGPu0e4=

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.

En este sentido, la DGTI ha informado que parte del documento requerido debe ser clasificado como **reservado**, por contener información clasificada como reservada, consistente en los "Resultados de evaluación de riesgos de seguridad informática" a los sistemas críticos de la Suprema Corte de Justicia de la Nación, de conformidad con el artículo 113, fracción VII, de la Ley General de Transparencia, al considerar que su difusión implicaría colocar en un estado de vulnerabilidad a la Suprema Corte de Justicia de la Nación, ya que al entregar dicha información se comprometería la seguridad informática de los sistemas y equipos de este Alto Tribunal, porque se pondría en riesgo la seguridad operativa de la infraestructura tecnológica que permite la operación de las diversas áreas del Alto Tribunal.

Además de que divulgar la información antes precisada podría proporcionar elementos que serían de utilidad para personas o grupos con intenciones delictivas lo que podría poner en riesgo la seguridad de este Alto Tribunal, así como menoscabaría la seguridad y certeza de los ciudadanos que acuden a esta Suprema Corte, por las razones siguientes:

- Permitiría el acceso ilícito a sus sistemas y equipos informáticos, intentando la suplantación de los mismos;

- Potenciaría la posibilidad de vulnerar la seguridad de su infraestructura tecnológica;

- Permitiría establecer con un alto grado de precisión la información técnica referente a los protocolos de seguridad y las características de la

bF/wOfIJfPkwcqbjfJjJUtZqEtFR938T4t0GuGPu0e4=

---

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."

infraestructura instalada;

- Pondría en un estado vulnerable a la institución, facilitando la intervención de las comunicaciones y permitiendo usurpar permisos requeridos en la red para obtener información;

- Daría a conocer puntos de vulnerabilidad para la seguridad de la infraestructura de cómputo;

- Vulneraría sus sistemas informáticos, así como la información contenida en éstos;

- Atentaría en contra de su infraestructura tecnológica, afectando el ejercicio de sus labores sustantivas; y

- Modificaría, destruiría o provocaría pérdida de información contenida en sus sistemas.

De igual forma, la entrega de “Resultados de evaluación de riesgos de seguridad informática”, podría ocasionar lo siguiente:

- La usurpación de sus permisos de acceso a sus sistemas críticos;

- La afectación de la disponibilidad de sus sistemas críticos, y

- El robo de la información que obra en sus sistemas críticos.

Al respecto, señaló que lo anteriormente expuesto se refuerza con lo resuelto por el Comité de Transparencia de la Suprema Corte de Justicia de la Nación, en las resoluciones de los expedientes CT-CUM-R/A-2-2019, derivado del CT-CI/A-27-2018, así como el diverso CT-CI/A-7-2020.

Por su parte, en relación con la información solicitada en el **punto 4**, la Unidad General de Transparencia, es el órgano que, entre otras atribuciones, cuenta con la de administrar el portal de transparencia y datos personales de este Alto Tribunal, así como implementar y mantener los mecanismos y sistemas electrónicos que permitan cumplir con las obligaciones y políticas en esas materias,

bF/wOflJfPkwcqbjfJjJUtZqEtFR938T4t0GuGPu0e4=

de conformidad con el artículo 40[9] del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación.

En ese sentido, ha informado que clasifica como reservada la información contenida en los anexos 1. Análisis de Riesgo 2022, 2. Análisis de Riesgo 2022, 3. Comparativo de brecha y 4: Análisis de brecha 2022, del Documento de seguridad 2023[10], en términos de la fracciones I y VII, del artículo 113 de la Ley General de Transparencia y 110, fracciones I y VII, de la Ley Federal de la materia, ya que de divulgarse, se vulnerarían las medidas de protección, lo que generaría la expectativa razonable de que ocurra un ataque intrusivo a las bases de datos personales en posesión de este Alto Tribunal pudiendo, incluso, afectar el desempeño de la función jurisdiccional y de las áreas administrativas de este Alto Tribunal.

bF/wOfIJfPkwcqbjfJjlJUtZqEtFR938T4t0GuGPu0e4=

---

[9] "**Artículo 40.** La Unidad General de Transparencia y Sistematización de la Información Judicial tendrá las atribuciones siguientes:
I. Administrar, recibir y difundir la información que involucre a la Suprema Corte en el ámbito de las obligaciones de transparencia, comunes y específicas, así como propiciar su actualización conforme a las disposiciones jurídicas aplicables;
II. Promover e implementar, previa aprobación de la o el Presidente, las políticas y acciones de transparencia proactiva;
III. Administrar el portal de transparencia y datos personales de la Suprema Corte, así como implementar y mantener los mecanismos y sistemas electrónicos que permitan cumplir con las obligaciones y políticas en esas materias;
IV. Recibir, dar trámite y desahogar las solicitudes de acceso a la información, así como las de acceso, rectificación, cancelación u oposición a la publicación de datos personales que obren en los archivos de la Suprema Corte; notificar a los solicitantes las determinaciones emitidas en los procedimientos correspondientes y, en su caso, entregar la información requerida, así como desahogar los medios de impugnación que se interpongan;
V. Auxiliar a los particulares en la elaboración de solicitudes de acceso a la información, así como las de acceso, rectificación, cancelación u oposición a la publicación de datos personales y, en su caso, orientarlos sobre los sujetos obligados que pudieran tener la información requerida;
VI. Proponer los procedimientos internos que aseguren la mayor eficiencia en la gestión de las solicitudes de acceso a la información, así como las de acceso, rectificación, cancelación u
oposición a la publicación de datos personales;
VII. Llevar un registro de las solicitudes, respuestas, resultados, costos de reproducción y envío;
VIII. Administrar y coordinar las acciones y procedimientos de transparencia, acceso a la información y protección de datos personales en todos los módulos instalados para ese efecto, y supervisar sus actividades mediante visitas técnicas en las sedes bajo su adscripción;
IX. Asesorar a los órganos y áreas para la publicación de la información que constituye obligación de transparencia; la atención de las solicitudes de información o de acceso, rectificación, cancelación u oposición de datos personales; la clasificación, conservación y resguardo de cualquier documento que contenga información reservada o confidencial, y la protección de los datos personales bajo su resguardo;
X. Hacer del conocimiento de la instancia competente la probable responsabilidad por el incumplimiento de las obligaciones previstas en las disposiciones aplicables;
XI. Fungir como vínculo o enlace con otros sujetos obligados y con el organismo garante federal en materia de transparencia, acceso a la información y protección de datos personales;
XII. Proponer planes de capacitación en la materia de transparencia, acceso a la información y protección de datos personales;
XIII. Generar información cuantitativa y cualitativa sistematizada, exhaustiva y confiable sobre los asuntos jurisdiccionales y la actividad institucional de la Suprema Corte;
XIV. Generar informes y reportes estadísticos a solicitud de la Presidencia o de las Ministras y Ministros de la Suprema Corte;
XV. Desarrollar y mantener actualizado un portal interactivo de sistematización de la información judicial accesible a la ciudadanía, y
XVI. Publicar en el portal de estadística judicial la información sobre seguimiento de casos, indicadores de gestión jurisdiccional y actividad institucional de la Suprema Corte."
[10] Aprobado en la Décima Cuarta Sesión del Comité de Transparencia celebrada el 9 de agosto de 2023.

Ello, en tanto que el análisis de riesgo que se desarrolla en el Documento de Seguridad 2023, identifica los diversos factores de riesgo a que están expuestos los tratamientos de datos personales y calcula el riesgo latente de cada uno de ellos; y, en el análisis de brecha, identifica la distancia que existe entre las medidas recomendadas y las medidas implementadas por cada uno de los tratamientos reportados, es decir, ubica las medidas de seguridad que hacen falta implementar para el resguardo de los datos personales y cuyos resultados dan sustento a las políticas y mecanismos institucionales en materia de protección de datos personales.

Es así que con la reserva se busca proteger la información y las bases de datos personales, evitando exponerlas a un ataque que pudiera conseguir vulnerarlas u obtenerlas para beneficiarse de ellas, lo que pondría en riesgo la privacidad de las personas titulares y podría ser causa de responsabilidad de la Suprema Corte de Justicia de la Nación, en términos de los deberes y las causas de incumplimiento de las obligaciones, especialmente de las vulneraciones previstas en los artículos 38 y 41 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Por tanto, su divulgación representa un riesgo real, demostrable e identificable de perjuicio significativo a la seguridad de la información y al derecho de protección de datos personales de los titulares de dicha información, ante lo cual no puede prevalecer el interés particular del peticionario, sino un interés mayor de proteger esa información.

A mayor abundamiento, señaló que se actualiza el supuesto de reserva previsto en la fracción I del artículo 113 de la Ley General de Transparencia, pues divulgar “los niveles de riesgo identificados” y “el análisis de brecha” contenidos en los anexos del Documento de Seguridad 2023, podría vulnerar el derecho a la protección de datos personales en posesión de la Suprema Corte de Justicia de la Nación, ya que se conocería el nivel y las medidas de protección implementadas por este Alto Tribunal para cada uno de los tratamientos de datos personales que se encuentran bajo su resguardo, así como el grado de vulnerabilidad de la institución en materia de seguridad de la información y las capacidades institucionales de reacción para enfrentar el mal uso de los datos personales que se encuentran bajo resguardo de este Alto Tribunal, lo que actualiza el supuesto de

bF/wOflJfPkwcqbjfJjJUtZqEtFR938T4t0GuGPu0e4=

reserva contenido en la fracción VII del artículo 113 de la citada Ley General de Transparencia.

Sobre las consideraciones que exponen las áreas vinculadas, se estima que en el caso se actualiza la clasificación de parcialmente reservada de los documentos Manual del Sistema de Gestión de Seguridad de la Información de este Alto Tribunal y Documento de seguridad 2023, conforme a las causales de reserva previstas en las fracciones I y VII del artículo 113 de la Ley General, así como sus correlativas del artículo 110 de la Ley Federal, los cuales disponen:

> *"**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;*
> *[…]*
> ***VII.** Obstruya la prevención o persecución de los delitos […]"*
>
> *"**Artículo 110.** Conforme a lo dispuesto por el artículo 113 de la Ley General, 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;*
> *[…]*
> ***VII.** Obstruya la prevención o persecución de los delitos […]"*

Lo anterior se estima así, pues en relación con el alcance de la fracción I de los preceptos antes transcritos, de conformidad con el artículo décimo octavo de los *"Lineamientos generales en materia de clasificación y desclasificación de la información",* se considera un riesgo a la seguridad pública la divulgación de aquella información que pueda poner en riesgo las funciones a cargo de la Federación 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.

Luego, sobre el artículo 110, fracción VII, de la Ley Federal de Transparencia, cuyo contenido es idéntico al que dispone la Ley General de Transparencia en el artículo 113, fracción VII, se tiene presente la resolución emitida por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) en el recurso de revisión 10276/18[11], derivado de la diversa clasificación CT-CI/A-27-2018[12], cumplimentada por este Comité en la resolución

[11] Consultable en: consultas.ifai.org.mx/Sesiones
[12] Disponible en: Clasificación CT-CI-A-27-2018 (scjn.gob.mx)

bF/wOflJfPkwcqbjfJjlUtZqEtFR938T4t0GuGPu0e4=

CT-CUM-R/A-2-2019[13], en la que se señaló que *"como información reservada podrá clasificarse aquella cuya 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 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, agregando que: *"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"*, considerando 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".*

En virtud de lo anterior, en la resolución del INAI se argumenta que *"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 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 tanto, que es procedente su reserva, de conformidad con el precepto jurídico que se analiza.

En estrecha relación con la clasificación que realiza la DGTI, se tiene en cuenta lo argumentado por este Comité en la resolución de cumplimiento CT-CI/A-

[13] Disponible en: CT-CUM-R-A-2-2019.pdf (scjn.gob.mx)

bF/wOflJfPkwcqbjfJjJUtZqEtFR938T4t0GuGPu0e4=

7-2020[14], en la que, entre otros aspectos se determinó que la información relativa a las políticas de vulnerabilidad implementadas para la prevención y solución de amenazas conforme a cada elemento para la protección de los sistemas constituye información susceptible de ser clasificada como reservada, en tanto que esa área informó que con su acceso se ponían en riesgo los sistemas de datos de este Alto Tribunal que no son públicos, ya que se daría a conocer información técnica sobre los equipos de cómputo, los protocolos de seguridad y las características de la infraestructura instalada.

Asimismo, se considera pertinente citar la resolución CT-CI/A-2-2020[15], en la que este Comité confirmó la clasificación de información semejante a la que se analiza ahora, esto es, los apartados relativos al análisis de riesgo y al análisis de brecha del Documento de seguridad 2019, al considerar que su divulgación vulneraría las medidas de protección generando la expectativa razonable de que ocurriera un ataque intrusivo a las bases de datos personales en posesión de este Alto Tribunal, pudiendo, incluso, afectar el desempeño de la función jurisdiccional y de las áreas administrativas de este Alto Tribunal.

En este contexto, este Comité estima que las razones expuestas por las instancias vinculadas para motivar la reserva parcial de los documentos que se analizan en este apartado, actualizan las hipótesis de reserva que prevé el artículo 113, fracciones I y VII, de la Ley General de Transparencia, en tanto que divulgar en su integridad el Manual del Sistema de Gestión de Seguridad de la Información así como el Documento de seguridad 2023 de este Alto Tribunal, implicaría colocar a la Suprema Corte de Justicia de la Nación en un estado de vulnerabilidad al poner en riesgo la seguridad operativa de la infraestructura tecnológica que permite la operación de la función jurisdiccional y de las diversas áreas administrativas que la conforman, pues se genera la expectativa razonable de que ocurra un ataque intrusivo que pudiera inhabilitar el uso y funcionamiento de las medidas implementadas, tanto para resguardar la seguridad informática de los sistemas y equipos de este Alto Tribunal, como para proteger la confidencialidad e integridad de los datos personales que posee la institución; de ahí que dichas razones justifican su reserva.

bF/wOflJfPkwcqbjfJjJUtZqEtFR938T4t0GuGPu0e4=

[14] Disponible en: CT-CI-A-7-2020 (scjn.gob.mx)
[15] Disponible en: CT-CI-A-2-2020 (scjn.gob.mx)

En esta línea de pensamiento, se estima que de igual forma se justifica la reserva parcial de los documentos que se analizan desde la perspectiva de la seguridad pública, pues constituye una razón de peso para acotar el derecho de acceso a la información, tomando en consideración que la divulgación de las evaluaciones y resultados de riesgo contenidas en los documentos que se analizan, reflejarían el grado de vulnerabilidad de esta institución en materia de seguridad de protección de datos personales así como comprometería la información que obra en los archivos digitales de este Alto Tribunal, lo que se reitera, representa un riesgo real para la seguridad pública y de las personas que acuden a este Alto Tribunal para ejercer sus derechos y obtener certeza en la impartición de justicia.

Prueba de daño

En concordancia con los argumentos señalados, se estima que, como lo plantea la DGTI, existe un riesgo real, demostrable e identificable de perjuicio significativo al interés público y a la seguridad pública en general, respecto a la difusión de los “Resultados de evaluación de riesgos de seguridad informática” (correspondientes al Manual del Sistema de Gestión de Seguridad de la Información), sobre los sistemas críticos de la Suprema Corte de Justicia de la Nación, ya que implicaría colocar en un estado de vulnerabilidad a la institución, por lo que entregar dicha información comprometería la seguridad informática de los sistemas y equipos de este Alto Tribunal, en virtud de que se pondría en riesgo la seguridad operativa de la infraestructura tecnológica que permite la operación de las diversas áreas y órganos que lo conforman.

Además, la DGTI sostuvo que el daño que podría producirse con la publicidad de la información es mayor que el interés de conocerla, por lo que su reserva se adecua al principio de proporcionalidad, en tanto que el resguardo de la información precisada implica llevar a cabo la prevención del delito de acceso ilícito a sistemas y equipos de informática tipificado en el Código Penal Federal, lo cual cobra importancia si se considera que dicha conducta podría implicar conocer, copiar, modificar, destruir o provocar la pérdida de información contenida en sistemas o equipos de informática, por lo que revelar los “Resultados de evaluación de riesgos de seguridad informática” a los sistemas críticos de la Suprema Corte de Justicia de la Nación no sólo comprometería la información que obra en los archivos

bF/wOflJfPkwcqbjfJjlJUtZqEtFR938T4t0GuGPu0e4=

digitales del sujeto obligado, sino que menoscabaría la seguridad y certeza de los ciudadanos que acuden a este Alto Tribunal.

Por su parte, en relación con los anexos 1 a 4 del Documento de seguridad 2023, los cuales corresponden al “análisis de riesgo” y al “análisis de brecha” del propio Documento de Seguridad, la divulgación de esa información sí puede vulnerar el derecho a la protección de datos personales en posesión de este Alto Tribunal, pues como se ha señalado, podría poner en riesgo la estrategia de seguridad implementada para proteger los datos personales que se encuentran bajo su resguardo, al divulgarse los niveles de riesgo identificados en los tratamientos de datos personales y, con el análisis de la brecha, se daría a conocer el grado de vulnerabilidad de esta institución en materia de seguridad de protección de datos personales, lo que, se reitera, representa un riesgo real para la seguridad pública y de las personas.

Además, como se estableció previamente, la reserva de la información busca proteger la seguridad de la información y el derecho de protección de datos personales de los titulares de dicha información, ante lo cual no puede prevalecer el interés particular de la persona solicitante, sino un interés mayor de proteger esa información, por lo que la medida cuenta con una finalidad válida, ya que busca tutelar otros valores de rango constitucional.

La reserva es idónea, porque con ello se evita la vulneración o indebido tratamiento que pudieran recibir los datos personales que tiene en resguardo este Alto Tribunal, comprometiendo con ello la seguridad de la información y el derecho a la protección de datos personales de los titulares, pues su difusión puede poner en peligro la integridad y el ejercicio de los derechos de las personas, de ahí que la reserva es apta y contribuye al fin perseguido.

Además, no existe un medio alternativo que pudiera garantizar el derecho de acceso a la información respecto de la información reservada, sin que implique, en alguna medida, un riesgo para los valores protegidos por la misma. No obstante, la entrega de la versión pública del Documento de seguridad 2023 sin sus anexos se erige como el medio menos restrictivo que consigue balancear el derecho de acceso a la información y los valores protegidos por la reserva.

bF/wOflJfPkwcqbjfJjlUtZqEtFR938T4t0GuGPu0e4=

Por último, se estima que la reserva es proporcional a la acotación del acceso a la información pública, pues se busca proteger las bases de datos personales que obran en resguardo de este Alto Tribunal, evitando exponerlas a un ataque que pudiera conseguir vulnerarlas u obtenerlas para beneficiarse de ellas, lo que podría poner en riesgo la privacidad de las personas titulares, ante lo cual debe rendirse el interés público de acceso a esa información en particular.

En mérito de lo hasta aquí expuesto, se justifica la reserva de la información consistente en los “Resultados de evaluación de riesgos de seguridad informática” en el Manual del Sistema de Gestión de Seguridad de la Información, así como de los anexos 1 a 4 del Documento de seguridad 2023, pues su clasificación constituye el medio menos lesivo para la adecuada protección del bien jurídico tutelado, como es la seguridad pública general, de ahí que no puede prevalecer el interés particular de la persona solicitante al requerir esa información.

Plazo de reserva

Ahora bien, en el caso específico, en términos de lo señalado en el artículo 101[16] de la Ley General de Transparencia, se determina que el plazo de reserva sea por cinco años, ya que acorde con las consideraciones expuestas por las instancias vinculadas, dicho plazo es proporcional a la naturaleza y al grado de especificidad del tipo de información de que se trata.

En tales circunstancias, se encomienda a la Unidad General de Transparencia que ponga a disposición de la persona solicitante las versiones

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

bF/wOflJfPkwcqbjfJjJUtZqEtFR938T4t0GuGPu0e4=

públicas del Manual del Sistema de Gestión de Seguridad de la Información que proporciona la DGTI, así como del Documento de seguridad 2023, sin sus anexos.

Por lo expuesto y fundado, se

R E S U E L V E:

PRIMERO. Se tiene por atendida la solicitud respecto de la información analizada en el apartado 1 del considerando segundo de la presente resolución.

SEGUNDO. Se confirma la clasificación como reservada de la información solicitada, en los términos del apartado 2 del considerando segundo de esta resolución.

Notifíquese a la persona solicitante, a las instancias requeridas y a la Unidad General de Transparencia y, en su oportunidad, archívese como asunto concluido.

Así, por unanimidad de votos, lo resolvió el Comité de Transparencia de la Suprema Corte de Justicia de la Nación y firman el Licenciado Mario José Pereira Meléndez, Director General de Asuntos Jurídicos y Presidente del Comité; el Maestro Christian Heberto Cymet López Suárez, Contralor del Alto Tribunal y, el Licenciado Adrián González Utusástegui, Titular de la Unidad General de Investigación de Responsabilidades Administrativas; integrantes del Comité, ante 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

bF/wOfIJfPkwcqbjfJjjUtZqEtFR938T4t0GuGPu0e4=

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."

bF/wOflJfPkwcqbjfJjJUtZqEtFR938T4t0GuGPu0e4=

Firmado por: CHRISTIAN HEBERTO CYMET LOPEZ SUAREZ
No. serie: 641779741797661081599202748245712497442704864255
Fecha: 13/09/2023 11:32:32.1720000 a. m.

Firmado por: SELENE GONZALEZ MEJIA
No. serie: 641779741797661077637794622532495617765507521176
Fecha: 06/09/2023 05:14:25.8030000 p. m.

Firmado por: MARIO JOSE PEREIRA MELENDEZ
No. serie: 641779741797661077637794622532495617765507529726
Fecha: 06/09/2023 05:43:08.3590000 p. m.

Firmado por: ADRIAN GONZALEZ UTUSASTEGUI
No. serie: 641779741797661077637794622532495617765507514581
Fecha: 06/09/2023 08:08:47.7330000 p. m.