ATENTA NOTA AL DIRECTOR GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN

ASUNTO: Atención al oficio número UGTSIJ/TAIPDP-3829-2023 referente a la solicitud de información con folio PNT 330030523001697 y folio interno UT-A/0487/2023, en los que se requiere lo siguiente:

> *"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. Que estándar para la seguridad de la información se tiene implementado en la institución? (…)"* (sic)

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 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 VII 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

[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

2bCvKHKPro0khctHuxmxXqKbndyea93S6YJPnj7GvOk=

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 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

ARTICULO 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.

2bCvKHKPro0khctHuxmxXqKbndyea93S6YJPnj7GvOk=

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.

ARTICULO 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.

ARTICULO 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:

2bCvKHKPro0khctHuxmxXqKbndyea93S6YJPnj7GvOk=

(…)
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 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.*

2bCvKHKPro0khctHuxmxXqKbndyea93S6YJPnj7GvOk=

- *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 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

2bCvKHKPro0khctHuxmxXqKbndyea93S6YJPnj7GvOk=

aseguramiento, la confidencialidad, integridad y disponibilidad de los datos y de la información, así como de los sistemas que la procesan.

Sin otro particular, hago propicia la ocasión para enviarle un cordial saludo.

Rol	Nombre y Cargo	Firma	Rúbrica
Revisó:	**Mtro. Omar Salinas García** Director de Seguridad Informática		
Elaboró	**Mtro. Ramón Caballero Ledesma** Subdirector de Cumplimiento de Seguridad Informática		

El presente documento se firma digitalmente de conformidad a lo establecido en el artículo 3 del Acuerdo General de Administración III/2020, del Presidente de la Suprema Corte de Justicia de la Nación, del 17 de septiembre de 2020, por el que se regula el trámite electrónico y uso de la firma electrónica certificada del Poder Judicial de la Federación (FIREL) para actuaciones administrativas.

2bCvKHKPro0khctHuxmxXqKbndyea93S6YJPnj7GvOk=

Firmado por: RAMON CABALLERO LEDESMA
No. serie: 641779741797661077637794622532495617765507495339
Fecha: 09/08/2023 05:59:00.2200000 p. m.

Firmado por: OMAR SALINAS GARCIA
No. serie: 641779741797661081599202748245712497442704856788
Fecha: 09/08/2023 06:40:15.9350000 p. m.