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

INEXISTENCIA DE INFORMACIÓN
CT-I/A-18-2021

INSTANCIAS REQUERIDAS:

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 **ocho de septiembre de dos mil veintiuno.**

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

I. Solicitud de información. El dos de agosto de dos mil veintiuno, se recibió en la Plataforma Nacional de Transparencia la solicitud tramitada con el folio 0330000131221, en la que se requiere:

> *"1. Informar sí (sic) dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan;*
> *2. Informar sí (sic) es que se cuenta con una estrategia de ciberseguridad dentro de la institución, en caso de respuesta afirmativa, informar lo siguiente (i) referir la fecha de creación; (ii) la fecha de implementación, (iii) sí es que se ha actualizado o modificado y en cuántas ocasiones; (iv) cuáles áreas participaron en la creación de dicha estrategia;*
> *3. Informar sí se cuenta con un sistema de gestión de seguridad de la información dentro de la institución;*
> *4. Informar sí de conformidad con la Ley General de Protección de Datos Personales en Posesión de Particulares se cuenta con lo siguiente Un sistema de gestión de protección de datos personales, en caso de ser afirmativa esta pregunta, ¿desde cuándo se adoptó y cuáles áreas participaron en su desarrollo e implementación?;*
> *5. Informar sí es que se cuenta con un plan de continuidad del negocio, para el caso de algún evento o incidente de seguridad cibernética o física e informar desde cuándo se implementó;*
> *6. Informar sí se cuenta con un modelo o sistema de comunicación, para informar a la sociedad en general sobre los eventos o incidentes de seguridad de la institución, y en caso de ser afirmativo, ¿cuáles áreas de la institución que participan? e informar desde cuándo se implementó;*
> *7. Informar sobre sí se cuenta con un modelo o sistema de comunicación para informar a los titulares de datos personales en caso de brechas de seguridad de esta información, y señalar cuáles áreas de la organización participan en su implementación y desde cuándo se implementó;*

8. Informar sí se realiza capacitación continua a los servidores públicos en materia de ciberseguridad y cada cuándo se lleva a cabo, así como los temas que se abordan;
9. Informar sí se cuenta con un procedimiento en caso de detección de alguna amenaza o vulneración de seguridad y cuál es el área encargada de atender los reportes;
10. Informar sí se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos;
11. Informar sí las personas encargadas de sistemas de información, donde se brinde información pública, cuentan con conocimientos comprobables en las siguientes materias (i) transparencia; (ii) protección de datos personales; (iii) archivos públicos; o, (iv) seguridad de la información.
12. Informar sí han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas;
13. Informar sí se cuenta con un modelo de madurez de seguridad de la información o ciberseguridad dentro de la institución, en caso afirmativo informar desde cuándo se implementa;
14. Informar sí se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son;
15. Informar sí algún sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que se emplee implica el tratamiento intensivo y/o relevante de datos personales, de conformidad de la ey en la materia; en caso afirmativo señalar sí se han llevado a cabo evaluaciones de impacto en materia de protección de datos personales; señalar cuáles han sido las recomendaciones vertidas por el del INAI, en su caso;
16. Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución;
17. Informar sí se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad;
18. Señalar si se cuenta con un sistema de gestión de incidentes y cuáles áreas de la institución participan en este;
19. Señalar si se cuenta con un help desk que recoja las incidencias reportadas por los servidores públicos, y en su caso señalar si es interno o externo.
20. Señalar si se cuenta con un equipo de respuesta a incidentes cibernéticos, especificar si es interno o externo." [Sic].

II. Acuerdo de admisión de la solicitud. En acuerdo de cinco de agosto de dos mil veintiuno, la Unidad General de Transparencia y Sistematización de la Información Judicial (Unidad General de Transparencia), por conducto de su Subdirector General, una vez analizada la naturaleza y contenido de la solicitud, con fundamento en los artículos 123 y 124, de la Ley General de Transparencia y Acceso a la Información Pública, 124 y 125, de la Ley Federal de Transparencia y Acceso a la Información Pública y 7 del Acuerdo General de Administración 5/2015, la estimó procedente y ordenó abrir el expediente UT-A/0236/2021.

III. Requerimiento de información. El Titular de la Unidad General de Transparencia, a través del oficio UGTSIJ/TAIPDP/2327/2021, enviado mediante comunicación electrónica de nueve de agosto de dos mil veintiuno, solicitó a la

Dirección General de Tecnologías de la Información que se pronunciara sobre la existencia y clasificación de la información solicitada en los puntos **1 a 3, 5 y 6, 8 a 13 y 16 a 20.**

Asimismo, tomando en consideración que parte de la información requerida por el solicitante hace referencia a la Ley General de Protección de Datos Personales en Posesión de Particulares, y dado que la solicitud de mérito fue dirigida a este Alto Tribunal, se estimó que el requirente pretendió aludir a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, por lo que se instruyó dar vista a la Unidad General de Transparencia, a efecto de que se pronunciara respecto de la información de los **puntos 4, 7, 11, 14 y 15** de la solicitud.

IV. Ampliación del plazo. La Unidad General de Transparencia, mediante oficio UGTSIJ/TAIPDP/2640/2021, enviado por correo electrónico el veinticuatro de agosto de dos mil veintiuno, solicitó la ampliación del plazo de respuesta, respecto del cual por oficio CT-342-2021, la Secretaría Técnica comunicó la autorización de la ampliación del plazo aprobada por el Comité de Transparencia en sesión de esa fecha, misma que fue notificada a la persona solicitante el veinticinco de agosto siguiente.

V. Informe de la Dirección General de Tecnologías de la Información. El dieciséis de agosto de dos mil veintiuno, se recibió en la cuenta de correo electrónico habilitada para tales efectos por la Unidad General de Transparencia, el oficio DGTI/353/2021, al que se adjuntaron las notas de cumplimiento DGTI/DSI/12/2021, SGSI-I/24/2021 y SGST/DAC/7/2021, en las que se informa:

> *"**RESPUESTA A SOLICITUD***
> ***1. Informar sí dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan;***
> ***Respuesta:** Se cuenta con la Comisión Interna de Protección Civil y de Seguridad de la Suprema Corte de Justicia de la Nación, la cual fue creada mediante **"**ACUERDO GENERAL DE ADMINISTRACIÓN NÚMERO VI/2020, DEL PRESIDENTE DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN, DE NUEVE DE NOVIEMBRE DE DOS MIL VEINTE". A continuación, se proporciona el link a través del cual se puede consultar el instrumento normativo antes citado, mismo que incluye el nombre de las áreas que participan en el citado Comité:*
> *https://www.scjn.gob.mx/conoce-la-corte/marconormativo/public/api/download?fileName=AGA-VI-20-Comisi%C3%B3n-Protecci%C3%B3n-Civil-Seguridad-SCJN.pdf*

2. Informar sí es que se cuenta con una estrategia de ciberseguridad dentro de la institución, en caso de respuesta afirmativa, informar lo siguiente (i) referir la fecha de creación; (ii) la fecha de implementación, (iii) sí es que se ha actualizado o modificado y en cuántas ocasiones; (iv) cuáles áreas participaron en la creación de dicha estrategia;

Respuesta: *Si se cuenta con una estrategia de ciberseguridad en la SCJN, la cual fue informada a la Comisión Interna de Protección Civil y de Seguridad de la Suprema Corte de Justicia de la Nación, el día 13 de julio del año en curso. Dicha estrategia se encuentra en proceso de implementación y fue diseñada por la Dirección de Seguridad Informática.*

3. Informar sí se cuenta con un sistema de gestión de seguridad de la información dentro de la institución;

Respuesta: *Derivado de la creación de la Comisión Interna de Protección Civil y de Seguridad de la Suprema Corte de Justicia de la Nación, se encuentra en proceso de planeación e instrumentación del sistema de gestión de seguridad de la información.*

5. Informar sí es que se cuenta con un plan de continuidad del negocio, para el caso de algún evento o incidente de seguridad cibernética o física e informar desde cuándo se implementó;

Respuesta: *No se cuenta con la formalización de un plan de continuidad del negocio; no obstante, se tiene el diseño y modelo de dicho plan, considerando implementar a corto plazo. Lo anterior, sin perjuicio de las acciones que realiza la Dirección General de Tecnologías de la Información, con la finalidad de mantener la continuidad de la operación y disponibilidad de la información, ante cualquier incidente de seguridad que se pudiera presentar.*

6. Informar sí se cuenta con un modelo o sistema de comunicación, para informar a la sociedad en general sobre los eventos o incidentes de seguridad de la institución, y en caso de ser afirmativo, ¿cuáles áreas de la institución que participan? e informar desde cuándo se implementó;

Respuesta: *No se cuenta con un modelo o sistema de comunicación; no obstante, como parte de la comunicación institucional, lo que se realiza es que, en caso de que exista algún evento o incidente de seguridad informática que pudiera afectar los servicios tecnológicos que la SCJN ofrece a la sociedad, la Dirección General de Tecnologías de la Información informa tal situación a la Dirección General de Comunicación Social, quien a través de los medios de comunicación oficiales da a conocer la misma.*

8. Informar sí se realiza capacitación continua a los servidores públicos en materia de ciberseguridad y cada cuándo se lleva a cabo, así como los temas que se abordan;

Respuesta: *Se realiza la capacitación continua a través de pláticas de ciberseguridad a los usuarios de la SCJN, donde se abordan diversos temas (uso de contraseñas fuertes, antivirus, uso seguro de correo electrónico, phishing, entre otros). Asimismo, de manera mensual se envían mediante correo electrónico a todos los servidores públicos de la SCJN, diversos InfoTips en materia de Seguridad Informática, así como su difusión a través del portal de Intranet y el boletín de "La Corte informa"; ello, como parte de la campaña permanente de concientización.*

9. Informar sí se cuenta con un procedimiento en caso de detección de alguna amenaza o vulneración de seguridad y cuál es el área encargada de atender los reportes;

Respuesta: *Se cuenta con el procedimiento denominado "Respuesta a incidentes en seguridad de la información" y el área que se encarga de atender estos reportes es la Dirección de Seguridad Informática.*

10. Informar sí se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos;

Respuesta: *Dentro de la normatividad de tecnologías de la información y comunicación, particularmente en el AGA IV/2008, capítulo quinto, se establece lo relativo al traslado de equipos. A continuación, se proporciona el link a través del cual se puede consultar el instrumento normativo antes citado:* *https://www.scjn.gob.mx/sites/default/files/marco-normativo/disposiciones-caracter-gral-expedidas-scjn/acuerdos-administrativos/documento/2016-12/3_AGA_IV2008.pdf*

11. Informar si las personas encargadas de sistemas de información, donde se brinde información pública, cuentan con conocimientos comprobables en las siguientes materias (i) transparencia; (ii) protección de datos personales; (iii) archivos públicos; o, (iv) seguridad de la información.

Respuesta*: El personal adscrito a la Dirección General de Tecnologías de la Información, cuenta con conocimientos comprobables en las materias de transparencia y protección de datos personales; en algunos casos también cuentan con conocimiento en seguridad de la información y archivo.*

12. Informar sí han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas;

Respuesta: *No se han presentado brechas de ciberseguridad desde el año 2015 a la fecha.*

13. Informar sí se cuenta con un modelo de madurez de seguridad de la información o ciberseguridad dentro de la institución, en caso afirmativo informar desde cuándo se implementa;

Respuesta: *Derivado de la creación de la Comisión Interna de Protección Civil y de Seguridad de la Suprema Corte de Justicia de la Nación, se encuentra en proceso de planeación e instrumentación el modelo de madurez de seguridad de la información.*

16. Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución;

Respuesta: *Se actualizan de manera continua y permanente.*

17. Informar sí se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad;

Respuesta: *Del año 2019 a la fecha se han llevado a cabo tres revisiones internas de controles de seguridad; la periodicidad es anual.*

18. Señalar si se cuenta con un sistema de gestión de incidentes y cuáles áreas de la institución participan en este;

Respuesta: *Se cuenta con una herramienta para la gestión de incidentes; cuando son incidentes en materia de seguridad, éstos se canalizan a la Dirección de Seguridad Informática, quien es el área encargada de su atención.*

19. Señalar si se cuenta con un help desk que recoja las incidencias reportadas por los servidores públicos, y en su caso señalar si es interno o externo.

Respuesta: *Se cuenta con una mesa de servicios para la gestión de incidentes; cuando son incidentes en materia de seguridad, éstos se canalizan a la*

*Dirección de Seguridad Informática, quien es el área encargada de su atención**.** Dicha mesa de servicios es interna.*

20. Señalar si se cuenta con un equipo de respuesta a incidentes cibernéticos, especificar si es interno o externo.

Respuesta: *Se cuenta con el procedimiento denominado Respuesta a incidentes en seguridad de la información y el área que se encarga de atender estos reportes es la Dirección de Seguridad Informática. Todo ello, es interno."* [Sic].

VI. Informe de la Unidad General de Transparencia y Sistematización de la Información Judicial. Mediante oficio sin número el Subdirector General de la Unidad General de Transparencia presentó un informe en los términos siguientes:

*"Respecto al **requerimiento 4**, es necesario precisar que el sistema de gestión, tal como lo formula el artículo 34 de la Ley General en la materia, se ha entendido como un sistema dinámico y en constante actualización pues se configura por un conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales.*

En ese sentido, le informo que, como primera etapa del sistema de gestión, esta Unidad General en coordinación con la Dirección General de Tecnologías de la Información, concluyó con el diseño y la propuesta del Portal de Datos Personales, el cual fue puesto a consideración del Comité de Transparencia y liberada el día 5 de julio del presente año a través del enlace para su consulta https://datos-personales.scjn.gob.mx/. Este portal pretende consolidarse, en su momento, como el sistema de gestión de conformidad con el parámetro establecido en el artículo 34 de la Ley General en la materia.

Incluso, cabe destacar que el propio Comité de Transparencia, en su resolución CT-I/A-2-2021 (https://www.scjn.gob.mx/sites/default/files/resoluciones/2021-03/CT-I-A-2-2021.pdf), consideró como primera versión del sistema de gestión el repositorio albergado en el portal de internet institucional que tuviera como elementos: i) los insumos del Documento de Seguridad y ii) los resultados de la primera etapa del Plan de Trabajo, los cuales se encuentran albergados actualmente en el referido Portal de Datos Personales.

*Respecto del **requerimiento 7**, deben considerarse tres cuestiones:*

Primero, que este Alto Tribunal cuenta con un INSTRUCTIVO PARA REGISTRAR Y REPORTAR VULNERACIONES DE DATOS PERSONALES cuyo propósito es que las áreas de la Suprema Corte de Justicia de la Nación (SCJN) identifiquen y registren, adecuadamente, las vulneraciones que ocurran a la seguridad de los datos personales que tratan en sus actividades cotidianas y resguardan en sus archivos físicos y electrónicos, de conformidad con los artículos 37 y 40 de la Ley General.

Este documento se encuentra disponible para su consulta en el siguiente enlace: https://datos-personales.scjn.gob.mx/sites/default/files/medidas-de-seguridad/Instructivo-para-registrar-y-reportar-vulneraciones-de-datos-personales.pdf y fue elaborado en agosto de 2020 por parte de esta Unidad General.

Segundo, que por lo que refiere a las "brechas de seguridad de la información", le informo que la Ley General en la materia establece la necesidad de que las medidas

de seguridad se encuentren debidamente documentadas y, en particular, prevé la elaboración de un documento de seguridad (artículos 34 y 35).

El documento de seguridad es un instrumento que permite a los sujetos obligados conocer el estado de cosas, las áreas de oportunidad y las líneas de acción para subsanar y atender los riesgos identificados en materia de seguridad de datos personales. En ese sentido, la Ley establece la información básica que deberá contener dicho documento (artículo 35) entre las que se encuentra un análisis de brecha.

Por tanto, el DOCUMENTO DE SEGURIDAD DE LA SCJN contempla un análisis de brecha que identifica la distancia que existe entre las medidas recomendadas y las medidas implementadas por cada uno de los tratamientos reportados por las áreas administrativas (documento publicado en versión pública: https://datos-personales.scjn.gob.mx/sites/default/files/documentos-relevantes/Documento-Seguridad.pdf).

Tercero, que un "modelo o sistema de comunicación para informar a los titulares de datos personales en caso de brechas de seguridad", es información ***es inexistente*** *debido a que tampoco existe alguna disposición legal que establezca la obligación de generarlo.*

Sobre el ***requerimiento 11****, es necesario informarle que anualmente, se aprueba y desarrolla un Programa de capacitación institucional en materia de transparencia, acceso a la información y protección de datos personales (PAC). Este programa se imparte a personas adscritas a la UGTSIJ, enlaces de transparencia de los órganos y las áreas, responsables de Módulos de Información y Acceso a la Justicia a nivel nacional (MIAJ`s), personas de nuevo ingreso, además de responsables de seguridad en datos personales.*

En el PAC 2021, se aprobaron cinco líneas generales de acción de capacitación:

i) Para ofrecer seguimiento a los programas de capacitación que anteceden (2015, 2016, 2017, 2018, 2019 y 2020), la primera línea tiene como la finalidad homologar los conocimientos de los enlaces de transparencia, responsables de MIAJ´s e integrantes de la UGTSIJ, de modo que se propone continuar con la actualización del universo de servidores públicos que ha sido la base en años anteriores (actualmente 116) y promover que todos concluyan los 11 cursos básicos albergados en el Centro Virtual de Capacitación en Acceso a la Información y Protección de Datos Personales (CEVINAI). Con ello se abarcan las desviaciones originadas en la implementación de programas anteriores, así como las áreas de oportunidad que se generen durante el 2021 por altas, bajas o modificaciones del personal.

ii) La segunda línea atiende dos aspectos: i) actualización y conservación de la información publicada en el portal de transparencia del Alto Tribunal, así como en el Sistema de Portales de Transparencia (SIPOT); y, ii) mejora en los procesos internos de acceso a la información, particularmente tratándose de solicitudes que se refieren a información que no tiene la denominación precisa que se utiliza al solicitarla, pero existen alternativas documentales. Dichos temas se abordarán a través del diseño, elaboración y difusión de dos cápsulas de capacitación y/o cursos virtuales dirigidos a los enlaces de transparencia y/o responsables de publicar información.

iii) Como tercera línea de desarrollo y en consonancia con el Plan de trabajo en materia de protección de datos personales, se perfilaron dos actividades dirigidas a las personas designadas como responsables de seguridad en datos personales: i) diseñar, elaborar y difundir cuatro cápsulas de capacitación con los siguientes ejes temáticos: a) avisos de privacidad, b) documento de seguridad, c) portal de datos personales, y d) supresión de datos personales (los dos últimos se encontrarán sujetos a la liberación del portal y la aprobación de normativa en materia archivo administrativo); y, ii) diseñar e impartir un taller de

seguridad informática para la protección de datos personales en coordinación con la Dirección General de Tecnologías de la Información.

iv) *La cuarta línea se refiere a los cursos de inducción en materia de transparencia, acceso a la información, protección de datos personales y archivos, esto último en colaboración con el Centro de Documentación y Análisis, Archivo y Compilación de Leyes, para personas de nuevo ingreso o reingreso al Alto Tribunal que son propuestas por la Dirección General de Recursos Humanos o las áreas que así lo requieran. Estas sesiones se desarrollarán en formato presencial – virtual a través de la herramienta TEAMS.*

v) *Finalmente, la quinta línea está relacionada con la profesionalización de los integrantes de la UGTSIJ a través de un curso presencial a distancia en materia de transparencia, acceso a la información y protección de datos personales, con recursos previamente presupuestados y cuyos ejes temáticos versarán sobre protección de datos personales y transparencia judicial enfocada a políticas públicas jurisdiccionales. Lo anterior está sujeto a la aprobación del techo presupuestal correspondiente.*

En ese sentido, los referidos programas son los instrumentos que esta Unidad General utiliza para transmitir conocimiento, en distintos formatos y niveles de especialización, en materia de transparencia, protección de datos personales, archivos públicos y seguridad de la información, sin que sea posible identificar si las personas que lo reciben están a cargo de "sistemas de información en los que se brinde información pública", pues ello es una cuestión dinámica.

*Sobre el **requerimiento 14**, le informo que no se han adoptado esquemas de mejores prácticas conforme a los parámetros señalados en los artículos 72 y 73 de la Ley General en la materia, en virtud de que la implementación de la política institucional actualmente se guía por el PLAN DE TRABAJO EN MATERIA DE DATOS PERSONALES (https://datos-personales.scjn.gob.mx/documentos-relevantes), cuyos objetivos son:*

1. *Eliminar las brechas a través de la implementación de medidas de seguridad pendientes en cada uno de los tratamientos de datos personales identificados; y,*
2. *Consolidar y preservar los niveles de protección de los datos personales a través de mecanismos de monitoreo y revisión.*

Además, dichos esquemas son potestativos de los sujetos obligados conforme al artículo 72 que dice que el responsable podrá desarrollar o adoptar, en lo individual o en acuerdo con otros responsables, encargados u organizaciones, esquemas de mejores prácticas.

*Por lo anterior, la información relativa a esquemas de mejores prácticas, en términos de los artículos 72 y 73 de la Ley General en la materia, es **inexistente**.*

*Sobre el **requerimiento 15**, el artículo 75 de la propia Ley General en la materia define los tres supuestos que deben satisfacerse para determinar un tratamiento intensivo o relevante de datos personales: i) existan riesgos inherentes a los datos personales a tratar; ii) se traten datos personales sensibles; y, iii) se efectúen o pretendan efectuar transferencias de datos personales.*

*Cabe indicar que, a partir de las actividades realizadas hasta el momento por esta Unidad General para la implementación de las disposiciones legales en materia de protección de datos personales, así como los reportes remitidos por las áreas y los órganos de la SCJN con ese mismo propósito, no se ha determinado la vigencia de algún un tratamiento intensivo o relevante de datos personales en términos de las disposiciones legales de la materia, por tanto esta información es **inexistente**.*

Esta cuestión fue abordada, indirectamente, por el Comité de Transparencia en su resolución CT-I/A-2-2021 (https://www.scjn.gob.mx/sites/default/files/resoluciones/2021-03/CT-I-A-2-2021.pdf)

pues no se ha determinado la existencia de un tratamiento intensivo o relevante de datos personales.

Fundamento

Artículos 129 de la Ley General de Transparencia y Acceso a la Información Pública; 130, cuarto párrafo, de la Ley Federal de Transparencia y Acceso a la Información Pública; 16, segundo párrafo, 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 lineamentos 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. Vista a la Secretaría del Comité de Transparencia. Mediante comunicación electrónica de treinta de agosto de dos mil veintiuno, el Titular de la Unidad General de Transparencia, a través del oficio UGTSIJ/TAIPDP/2657/2021, remitió el expediente electrónico UT-A/0236/2021 a la Secretaría del Comité de Transparencia, con la finalidad de que se dictara la resolución correspondiente.

VIII. Acuerdo de turno. Mediante acuerdo de treinta de agosto de dos mil veintiuno, la Presidencia del Comité de Transparencia, con fundamento en los artículos 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública, 23, fracción II, y 27, del Acuerdo General de Administración 5/2015, ordenó integrar el expediente **CT-I/A-18-2021** y, conforme al turno correspondiente, remitirlo al titular de la Unidad General de Investigación de Responsabilidades Administrativas del Alto Tribunal, a fin de que presentara la propuesta de resolución, lo que se hizo mediante oficio CT-348-2021, enviado por correo electrónico en esa misma fecha.

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

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, 4 y 44, fracciones II y III, de la Ley General de Transparencia y Acceso a la Información Pública, 65, fracciones II y III, de la Ley Federal de Transparencia y Acceso a la Información Pública, así como 23, fracciones II y III, del Acuerdo General de Administración 5/2015.

II. Análisis de la solicitud. En la solicitud se pide información relacionada con aspectos de seguridad informática y protección de datos personales por parte de este Alto Tribunal, por lo que a continuación se realiza el análisis de las respuestas que emitieron la Dirección General de Tecnologías de la Información y la Unidad General de Transparencia y Sistematización de la Información Judicial, respecto de cada punto de la solicitud.

1. Informar si dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan.

La Dirección General de Tecnologías de la Información informa que se cuenta con la Comisión Interna de Protección Civil y de Seguridad de la Suprema Corte de Justicia de la Nación, la cual fue creada mediante Acuerdo General de Administración VI/2020, del Presidente de la Suprema Corte de Justicia de la Nación, de nueve de noviembre de dos mil veinte y, al efecto, proporciona la siguiente liga electrónica a través de la cual se puede descargar ese documento.
https://www.scjn.gob.mx/conoce-la-corte/marconormativo/public/api/download?fileName=AGA-VI-20-Comisi%C3%B3n-Protecci%C3%B3n-Civil-Seguridad-SCJN.pdf

Al respecto, se advierte, por una parte, conforme al artículo 3° de dicho Acuerdo que la Comisión Interna de Protección Civil y de Seguridad tiene por objeto determinar las acciones encaminadas a preservar y salvaguardar la vida, integridad física, seguridad y salud de las personas servidoras públicas y visitantes; la seguridad de los bienes muebles, acervos documentales, inmuebles y activos informáticos, así como procurar la continuidad de operaciones de la Suprema Corte.

Por la otra, el artículo 4° de dicho Acuerdo General establece que la Comisión se integra por las personas titulares de los órganos y áreas de la Suprema Corte siguientes: I. Oficialía Mayor, quien la presidirá; II. Coordinación de la Oficina de la Presidencia; III. Secretaría General de Acuerdos; IV. Dirección General de Seguridad; V. Dirección General de Recursos Humanos; VI. Dirección General de Presupuesto y Contabilidad; VII. Dirección General de Infraestructura Física; VIII. Dirección General de Tecnologías de la Información, y IX. Dirección General de Recursos Materiales; de ahí que con esta información **se atiende** lo requerido sobre este punto.

2. Informar si es que se cuenta con una estrategia de ciberseguridad dentro de la institución, en caso de respuesta afirmativa, informar a) fecha de creación, b) fecha de implementación, c) si es que se ha actualizado o modificado y en cuántas ocasiones y d) cuáles áreas participaron en la creación de dicha estrategia.

La Dirección General de Tecnologías de la Información señala que sí se cuenta con una estrategia de ciberseguridad en este Alto Tribunal, la cual fue diseñada por la Dirección de Seguridad Informática y se informó de la misma a la Comisión Interna de Protección Civil y de Seguridad de la Suprema Corte de Justicia de la Nación, el día trece de julio del año en curso, por lo que con base en esta información se **estima parcialmente atendido este punto**.

Ello es así, considerando que, si la Dirección General de Tecnologías de la Información comunica la existencia de una estrategia de seguridad, posiblemente resguarda información relacionada con la fecha de creación o implementación y las áreas que participaron, planteamientos que no se advierten ni derivan del informe proporcionado.

En consecuencia, a fin de atender integralmente la solicitud, se **requiere**, por conducto de la Secretaría Técnica, a la Dirección General de Tecnologías de la Información para que, en el plazo de cinco días siguientes a la notificación esta resolución, se pronuncie sobre la información relacionada con la fecha de creación o implementación de la estrategia de seguridad y las áreas que participaron.

3. Informar si se cuenta con un sistema de gestión de seguridad de la información dentro de la institución.

La Dirección General de Tecnologías de la Información señala que, derivado de la creación de la Comisión Interna de Protección Civil y de Seguridad de la Suprema Corte de Justicia de la Nación, se encuentra en proceso de planeación e instrumentación el sistema de gestión de seguridad de la información, por lo que la información solicitada en este punto es, hasta este momento, **inexistente.**

4. Informar si de conformidad con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados se cuenta con un sistema de

gestión de protección de datos personales y, en su caso, ¿desde cuándo se adoptó y cuáles áreas participaron en su desarrollo e implementación?

En el informe de la Unidad General de Transparencia se señala que el sistema de gestión, tal como lo formula el artículo 34[1] de la Ley General en la materia, se ha entendido como un sistema dinámico y en constante actualización pues se configura por un conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales.

En ese sentido, informa que, como primera etapa del sistema de gestión, esa Unidad General, en coordinación con la Dirección General de Tecnologías de la Información, concluyó con el diseño y la propuesta del Portal de Datos Personales, el cual fue puesto a consideración del Comité de Transparencia y liberado el día cinco de julio del presente año a través del siguiente enlace para su consulta https://datos- personales.scjn.gob.mx/

En consecuencia, se tiene por **atendido** lo solicitado por el peticionario en este aspecto, puesto que el objetivo de este portal es consolidarse como el sistema de gestión que establece el artículo 34 de la Ley General en la materia, habida cuenta que el propio Comité de Transparencia, en su resolución CT-I/A-2-2021[2], consideró como primera versión del sistema de gestión el repositorio albergado en el portal de internet institucional que tuviera como elementos: i) los insumos del documento de seguridad, y ii) los resultados de la primera etapa del plan de trabajo, los cuales se encuentran albergados actualmente en el referido Portal de Datos Personales que ya se encuentra en operación y del cual se advierte que integra diversos rubros orientados a establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales.

---

[1] **Artículo 34.** Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión. Se entenderá por sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, de conformidad con lo previsto en la presente Ley y las demás disposiciones que le resulten aplicables en la materia.

[2] Consultable en la siguiente liga electrónica: https://www.scjn.gob.mx/sites/default/files/resoluciones/2021-03/CT-I-A-2-2021.pdf

5. Informar si se cuenta con un plan de continuidad del negocio para el caso de algún evento o incidente de seguridad cibernética o física y desde cuándo se implementó.

La Dirección General de Tecnologías de la Información refiere que no cuenta con la formalización de un plan de continuidad del negocio, pero tiene el diseño y modelo de dicho plan, el cual está se implementará a corto plazo. Ello, sin perjuicio de las acciones que realiza la Dirección General de Tecnologías de la Información, con la finalidad de mantener la continuidad de la operación y disponibilidad de la información, ante cualquier incidente de seguridad que se pudiera presentar.

En consecuencia, si hasta este momento no se cuenta formalmente con el documento relativo al plan de continuidad, la información solicitada en este punto es **inexistente.**

6. Informar si se cuenta con un modelo o sistema de comunicación para informar a la sociedad sobre los eventos o incidentes de seguridad de la institución, y en caso de ser afirmativo, ¿cuáles áreas de la institución participan? e informar desde cuándo se implementó.

La Dirección General de Tecnologías de la Información indica que no se cuenta con un modelo o sistema de comunicación, por lo que la información solicitada en este punto es **inexistente,** en los términos solicitados por el particular.

No obstante, la instancia vinculada señala que como parte de la comunicación institucional, lo que se realiza es que, en caso de que exista algún evento o incidente de seguridad informática que pudiera afectar los servicios tecnológicos que la Suprema Corte de Justicia de la Nación ofrece a la sociedad, la Dirección General de Tecnologías de la Información informa tal situación a la Dirección General de Comunicación Social, quien a través de los medios de comunicación oficiales, da a conocer la misma.

7. Informar si se cuenta con un modelo o sistema de comunicación para informar a los titulares de datos personales en caso de brechas de seguridad de esta información, y señalar cuáles áreas de la organización participan en su implementación y desde cuándo se implementó.

Al respecto, la Unidad General de Transparencia informa que, en principio, este Alto Tribunal cuenta con un instructivo para registrar y reportar vulneraciones de datos personales, cuyo propósito es que las áreas de la Suprema Corte de Justicia de la Nación identifiquen y registren adecuadamente las vulneraciones que ocurran a la seguridad de los datos personales que tratan en sus actividades cotidianas y resguardan en sus archivos físicos y electrónicos, de conformidad con los artículos 37 y 40[3] de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, el cual se encuentra disponible para su consulta en el siguiente enlace: https://datos-personales.scjn.gob.mx/sites/default/files/medidas-de-seguridad/Instructivo-para-registrar-y-reportar-vulneraciones-de-datos-personales.pdf y fue elaborado en agosto de dos mil veinte por parte de esa Unidad General.

Por lo que refiere a las “brechas de seguridad de la información”, los artículos 34 y 35[4] de la Ley General en la materia establecen la necesidad de que las medidas de seguridad se encuentren debidamente documentadas y, en particular, prevé la elaboración de un documento de seguridad.

El documento de seguridad es un instrumento que permite a los sujetos obligados conocer el estado de cosas, las áreas de oportunidad y las líneas de acción para subsanar y atender los riesgos identificados en materia de seguridad de datos personales, el cual, entre la información básica que debe contener, se encuentra un análisis de brecha.

En ese sentido, el documento de seguridad de este Alto Tribunal contempla un análisis de brecha que identifica la distancia que existe entre las medidas recomendadas y las medidas implementadas por cada uno de los tratamientos

---

[3] **Artículo 37.** En caso de que ocurra una vulneración a la seguridad, el responsable deberá analizar las causas por las cuales se presentó e implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales si fuese el caso a efecto de evitar que la vulneración se repita.
Artículo 40. El responsable deberá informar sin dilación alguna al titular, y según corresponda, al Instituto y a los Organismos garantes de las Entidades Federativas, las vulneraciones que afecten de forma significativa los derechos patrimoniales o morales, en cuanto se confirme que ocurrió la vulneración y que el responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, a fin de que los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos.

[4] **Artículo 35.** De manera particular, el responsable deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente:
I. El inventario de datos personales y de los sistemas de tratamiento; II. Las funciones y obligaciones de las personas que traten datos personales; III. El análisis de riesgos; IV. El análisis de brecha; V. El plan de trabajo; VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y VII. El programa general de capacitación.

reportados por las áreas administrativas (documento publicado en versión pública: https://datos-personales.scjn.gob.mx/sites/default/files/documentos-relevantes/Documento-Seguridad.pdf).

No obstante, no existe disposición legal que establezca la obligación de generar un *"modelo o sistema de comunicación para informar a los titulares de datos personales en caso de brechas de seguridad"*, como el que refiere el solicitante, por lo que la información es **inexistente**.

8. Informar si se realiza capacitación continua a los servidores públicos en materia de ciberseguridad y cada cuando se lleva a cabo, así como los temas que se abordan.

La Dirección General de Tecnologías de la Información señala que sí se proporciona capacitación continua a los usuarios de la Suprema Corte de Justicia de la Nación a través de pláticas de ciberseguridad, en las que se abordan diversos temas como uso de contraseñas fuertes, antivirus, uso de correo electrónico seguro, phishing, entre otros. Asimismo, de manera mensual se envían diversos InfoTips en materia de Seguridad Informática mediante correo electrónico a todos los servidores públicos del Alto Tribunal, y se difunden a través del portal de Intranet y el boletín de "La Corte informa"; ello, como parte de la campaña permanente de concientización, por lo que con esta información **se atiende** lo solicitado en este punto.

9. Informar si se cuenta con un procedimiento en caso de detección de alguna amenaza o vulneración de seguridad y cuál es el área encargada de atender los reportes.

La Dirección General de Tecnologías de la Información señala que se cuenta con el procedimiento denominado "Respuesta a incidentes en seguridad de la información" y el área que se encarga de atender estos reportes es la Dirección de Seguridad Informática, con lo que **se atiende** lo solicitado en este punto.

10. Informar si se cuenta con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos.

La Dirección General de Tecnologías de la Información indica que en el Acuerdo General de Administración IV/2008, del dieciséis de mayo de dos mil ocho, del Comité de Archivo, Biblioteca e Informática, relativo al uso y aprovechamiento de los bienes y servicios informáticos de la Suprema Corte de Justicia de la Nación, particularmente en el capítulo quinto del título segundo, se establece lo relativo al traslado de equipos y pone a disposición del solicitante la liga electrónica en que se puede descargar ese documento.

https://www.scjn.gob.mx/sites/default/files/marco-normativo/disposiciones-caracter-gral-expedidas-scjn/acuerdos-administrativos/documento/2016-12/3_AGA_IV2008.pdf

Al respecto, la citada porción normativa establece:

> ***"DEL TRASLADO DE EQUIPOS DE CÓMPUTO***
>
> ***Artículo 14.*** *Informática es la única facultada para emitir oficios y/o pases de salidas de los equipos informáticos y, en su caso, hacerlo del conocimiento del área de seguridad que corresponda.*
>
> *En la autorización de la salida, deberá especificarse el mayor número de datos y características posibles sobre el bien, conteniendo como mínimo la descripción, marca, modelo, número de serie y/o de inventario, componentes modulares de relevancia, lugar hacia donde se traslada, fecha, hora, la razón o motivo de ello, nombre de las personas que autorizan y de la persona que lo trasladará.*
>
> *Respecto a los bienes informáticos portátiles (laptops) será obligación del usuario resguardar el bien con los cuidados necesarios, así como evitar el dejarlo fuera de su custodia en todo momento.*
>
> *De igual forma será su responsabilidad el buen uso del manejo de la información, con base en su ética profesional, ya que al ser un equipo portátil es susceptible de que la información sea sustraída del equipo y mal manejada."*

Sobre este aspecto se estima necesario agregar que el Acuerdo General de Administración número I/2020[5] de diecisiete de marzo de dos mil veinte, del Presidente de la Suprema Corte de Justicia de la Nación, emitido en el contexto de la emergencia sanitaria ocasionada por el virus SARS-CoV2 (COVID-19), en el cual se autoriza al personal de esta Suprema Corte el traslado a su domicilio de las

[5] Consultable en la liga electrónica: https://www.scjn.gob.mx/sites/default/files/acuerdos_presidenciales/documento/2020-08/acuerdo%20general%20administración%20I-2020%20equipos%20cómputo.pdf

computadoras portátiles (laptops) que tuvieran bajo su resguardo para continuar con sus funciones.

Por lo anterior, se **estima atendido** es punto de la solicitud y se **instruye** a la Unidad General de Transparencia que comunique al solicitante las ligas electrónicas para consultar el contenido de los ordenamientos jurídicos aquí analizados.

11. Informar si las personas encargadas de sistemas de información, en los que se brinda información pública, cuentan con conocimientos comprobables en las siguientes materias (i) transparencia, (ii) protección de datos personales, (iii) archivos públicos o (iv) seguridad de la información.

Al respecto, la Dirección General de Tecnologías de la Información indica que su personal sí cuenta con conocimientos comprobables en materia de transparencia y protección de datos personales, y en algunos casos también cuentan con conocimiento en seguridad de la información y archivo.

En complemento, la Unidad General de Transparencia informa que anualmente se aprueba y desarrolla un programa de capacitación institucional en materia de transparencia, acceso a la información y protección de datos personales (PAC), el cual se imparte a personas adscritas a la Unidad General de Transparencia y Sistematización de la Información Judicial, enlaces de transparencia de los órganos y las áreas de esta Suprema Corte, responsables de Módulos de Información y Acceso a la Justicia a nivel nacional (MIAJ`s), personas de nuevo ingreso y a los responsables de seguridad en datos personales.

Señala que en el PAC 2021, se aprobaron cinco líneas generales de acción de capacitación:

i) Para ofrecer seguimiento a los programas de capacitación que anteceden (2015, 2016, 2017, 2018, 2019 y 2020), la primera línea tiene como la finalidad homologar los conocimientos de los enlaces de transparencia, responsables de MIAJ´s e integrantes de la Unidad General de Transparencia, de modo que se propone continuar con la actualización del universo de servidores públicos que ha sido la base en años anteriores (actualmente 116) y promover que todos concluyan los

11 cursos básicos albergados en el Centro Virtual de Capacitación en Acceso a la Información y Protección de Datos Personales (CEVINAI), con lo que se abarcan las desviaciones originadas en la implementación de programas anteriores, así como las áreas de oportunidad que se generen durante el año dos mil veintiuno por altas, bajas o modificaciones del personal.

ii) La segunda línea atiende dos aspectos: i) actualización y conservación de la información publicada en el portal de transparencia del Alto Tribunal, así como en el Sistema de Portales de Transparencia (SIPOT), y ii) mejora en los procesos internos de acceso a la información, particularmente tratándose de solicitudes que se refieren a información que no tiene la denominación precisa que se utiliza al solicitarla, pero existen alternativas documentales. Dichos temas se abordarán a través del diseño, elaboración y difusión de dos cápsulas de capacitación y/o cursos virtuales dirigidos a los enlaces de transparencia y/o responsables de publicar información.

iii) Como tercera línea de desarrollo y en consonancia con el Plan de trabajo en materia de protección de datos personales, se perfilaron dos actividades dirigidas a las personas designadas como responsables de seguridad en datos personales: i) diseñar, elaborar y difundir cuatro cápsulas de capacitación con los siguientes ejes temáticos: a) avisos de privacidad, b) documento de seguridad, c) portal de datos personales, y d) supresión de datos personales (los dos últimos se encontrarán sujetos a la liberación del portal y la aprobación de normativa en materia archivo administrativo); y, ii) diseñar e impartir un taller de seguridad informática para la protección de datos personales en coordinación con la Dirección General de Tecnologías de la Información.

iv) La cuarta línea se refiere a los cursos de inducción en materia de transparencia, acceso a la información, protección de datos personales y archivos, esto último en colaboración con el Centro de Documentación y Análisis, Archivo y Compilación de Leyes, para personas de nuevo ingreso o reingreso al Alto Tribunal que son propuestas por la Dirección General de Recursos Humanos o las áreas que así lo requieran. Estas

sesiones se desarrollarán en formato presencial – virtual a través de la herramienta TEAMS.

v) Finalmente, la quinta línea está relacionada con la profesionalización de los integrantes de la Unidad General de Transparencia a través de un curso presencial a distancia en materia de transparencia, acceso a la información y protección de datos personales, con recursos previamente presupuestados y cuyos ejes temáticos versarán sobre protección de datos personales y transparencia judicial enfocada a políticas públicas jurisdiccionales. Lo anterior está sujeto a la aprobación del techo presupuestal correspondiente.

En ese sentido, los referidos programas son los instrumentos que esa Unidad General utiliza para transmitir conocimiento, en distintos formatos y niveles de especialización, en materia de transparencia, protección de datos personales, archivos públicos y seguridad de la información, sin que sea posible identificar si las personas que lo reciben están a cargo de “sistemas de información en los que se brinde información pública”, pues ello es una cuestión dinámica.

En consecuencia, con base en lo informado por las instancias requeridas se estima que esta información **atiende** lo requerido sobre este aspecto.

12. Informar si han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas.

La Dirección General de Tecnologías de la Información indica que no se han presentado brechas de ciberseguridad desde el año 2015 a la fecha, con lo que **se atiende** lo requerido en este punto.

13. Informar si se cuenta con un modelo de madurez de seguridad de la información o ciberseguridad dentro de la institución, en caso afirmativo informar desde cuándo se implementa.

La información requerida en este punto es **inexistente** (hasta este momento) en virtud de que la Dirección General de Tecnologías de la Información informa que derivado de la creación de la Comisión Interna de Protección Civil y de Seguridad de la Suprema Corte de Justicia de la Nación, se encuentra en proceso de planeación e instrumentación el modelo de madurez de seguridad de la información.

14. Informar si se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son.

La Unidad General de Transparencia informa que no se han adoptado esquemas de *"mejores prácticas"* conforme a los parámetros señalados en los artículos 72 y 73[6] de la Ley General en la materia, en virtud de que la implementación de la política institucional actualmente se guía por el plan de trabajo en materia de datos personales[7], cuyos objetivos son:

1. Eliminar las brechas a través de la implementación de medidas de seguridad pendientes en cada uno de los tratamientos de datos personales identificados; y,
2. Consolidar y preservar los niveles de protección de los datos personales a través de mecanismos de monitoreo y revisión.

Agrega que el citado artículo 72, establece que el responsable podrá desarrollar o adoptar, en lo individual o en acuerdo con otros responsables, encargados u organizaciones, esquemas de mejores prácticas, por lo que dichos esquemas son potestativos de los sujetos obligados; de ahí que la información requerida en este punto es **inexistente**.

---

[6] **Artículo 72.** Para el cumplimiento de las obligaciones previstas en la presente Ley, el responsable podrá desarrollar o adoptar, en lo individual o en acuerdo con otros responsables, encargados u organizaciones, esquemas de mejores prácticas que tengan por objeto: I. Elevar el nivel de protección de los datos personales; II. Armonizar el tratamiento de datos personales en un sector específico; III. Facilitar el ejercicio de los derechos ARCO por parte de los titulares; IV. Facilitar las transferencias de datos personales; V. Complementar las disposiciones previstas en la normatividad que resulte aplicable en materia de protección de datos personales, y VI. Demostrar ante el Instituto o, en su caso, los Organismos garantes, el cumplimiento de la normatividad que resulte aplicable en materia de protección de datos personales.
Artículo 73. Todo esquema de mejores prácticas que busque la validación o reconocimiento por parte del Instituto o, en su caso, de los Organismos garantes deberá: I. Cumplir con los parámetros que para tal efecto emitan, según corresponda, el Instituto y los Organismos garantes conforme a los criterios que fije el primero, y II. Ser notificado ante el Instituto o, en su caso, los Organismos garantes de conformidad con el procedimiento establecido en los parámetros señalados en la fracción anterior, a fin de que sean evaluados y, en su caso, validados o reconocidos e inscritos en el registro al que refiere el último párrafo de este artículo. El Instituto y los Organismos garantes, según corresponda, deberán emitir las reglas de operación de los registros en los que se inscribirán aquellos esquemas de mejores prácticas validados o reconocidos. Los Organismos garantes, podrán inscribir los esquemas de mejores prácticas que hayan reconocido o validado en el registro administrado por el Instituto, de acuerdo con las reglas que fije este último.

[7] Consultable en la siguiente liga electrónica (https://datos-personales.scjn.gob.mx/documentos-relevantes).

15. Informar si algún sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que se emplee, implica el tratamiento intensivo y/o relevante de datos personales, de conformidad con la ley en la materia, en caso afirmativo señalar si se han llevado a cabo evaluaciones de impacto en materia de protección de datos personales y, en su caso, cuáles han sido las recomendaciones vertidas por el INAI.

La Unidad General de Transparencia informa que el artículo 75 de la propia Ley General en la materia define los tres supuestos que deben satisfacerse para determinar un tratamiento intensivo o relevante de datos personales: i) existan riesgos inherentes a los datos personales a tratar; ii) se traten datos personales sensibles, y iii) se efectúen o pretendan efectuar transferencias de datos personales.

Bajo este contexto, precisa que a partir de las actividades realizadas hasta el momento por esa Unidad General para la implementación de las disposiciones legales en materia de protección de datos personales, así como los reportes remitidos por las áreas y los órganos de este Alto Tribunal con ese propósito, **no se ha determinado la vigencia de algún un tratamiento intensivo o relevante de datos personales** en los términos de las disposiciones legales de la materia y, por ese motivo, la información solicitada es **inexistente**.

Como señala la instancia vinculada, mediante precedente CT-I/A-2-2021[8], este Comité validó la inexistencia de la información relacionada con una petición similar a la que ahora se analiza.

16. Informar cada cuanto tiempo se actualizan las medidas de ciberseguridad dentro de la institución.

La Dirección General de Tecnologías de la Información informa que se actualizan de manera continua y permanente, de tal suerte que **se atiende** este punto de la solicitud.

[8] Resuelto en sesión de veintisiete de enero de dos mil veintiuno; consultable en: https://www.scjn.gob.mx/sites/default/files/resoluciones/2021-03/CT-I-A-2-2021.pdf

17. Informar sí se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad.

La Dirección General de Tecnologías de la Información informa que del año dos mil diecinueve a la fecha se han llevado a cabo tres revisiones internas de controles de seguridad y la periodicidad es anual, con lo cual se tiene por **atendido** este planteamiento.

18. Señalar si se cuenta con un sistema de gestión de incidentes y cuáles áreas de la institución participan en este.

La Dirección General de Tecnologías de la Información informa que se cuenta con una herramienta para la gestión de incidentes y cuando implican cuestiones en materia de seguridad éstos se canalizan a la Dirección de Seguridad Informática, que es instancia responsable de su atención, por lo que se tiene por **atendido** este punto de la solicitud.

19. Señalar si se cuenta con un help desk que recoja las incidencias reportadas por los servidores públicos, y en su caso señalar si es interno o externo.

La Dirección General de Tecnologías de la Información indica que cuenta con una mesa de servicios para la gestión de incidentes y cuando implican incidentes en materia de seguridad éstos se canalizan a la Dirección de Seguridad Informática, que es la instancia responsable su atención**.** Asimismo, se comunica que la mesa de servicios es interna, por lo que con ello **se atiende** este aspecto de la solicitud.

20. Señalar si se cuenta con un equipo de respuesta a incidentes cibernéticos, especificar si es interno o externo.

La Dirección General de Tecnologías de la Información informa que cuenta con el procedimiento denominado “Respuesta a incidentes en seguridad de la información” y el área que se encarga de atender estos reportes es la Dirección de Seguridad Informática. Asimismo, se comunica que este procedimiento se realiza de manera interna, por tanto, con esta información **se atiende** este punto de la solicitud.

Ahora bien, como corolario de lo antes expuesto este Comité determina lo siguiente:

1) Información que se pone a disposición

Se estima que están **atendidos los puntos 1, 4**, **8, 9, 10**, **11, 12, 16, 17, 18, 19 y 20.** Por otra parte, está **parcialmente atendido el punto 2,** puesto que se informó sobre la existencia de una estrategia de seguridad institucional.

En consecuencia, se **instruye** a la Unidad General de Transparencia que ponga a disposición esta información al solicitante y los enlaces electrónicos que se proporcionaron para que pueda consultar la información.

2) Información inexistente

La **Dirección General de Tecnologías de la Información** decretó la inexistencia de la información respecto de los puntos 3 (sistema de gestión de seguridad), 5 (plan de continuidad del negocio), 6 (modelo de comunicación de incidentes de seguridad) y 13 (modelo de madurez de seguridad), puesto que no se cuenta con los mecanismos solicitados y, en otros casos, están en proceso su planeación y desarrollo.

Por su parte, **la Unidad General de Transparencia y Sistematización de la Información Judicial** se pronuncia por la inexistencia de la información de los puntos 7 (sistema de comunicación de brechas de seguridad), 14 (mejores prácticas en datos personales) y 15 (sistemas que utilicen tratamiento intensivo de datos personales).

Para analizar dichos pronunciamientos, cabe recordar que, conforme al esquema de nuestro sistema constitucional, el derecho de acceso a la información encuentra cimiento a partir de lo dispuesto en el artículo 6º, apartado A, de la Constitución Política de los Estados Unidos Mexicanos, cuyo contenido deja claro que, en principio, todo acto de autoridad es de interés general y, por ende, es susceptible de ser conocido por todos.

El acceso a la información pública comprende el derecho a solicitar, investigar, difundir, buscar y recibir información, **que se encuentre integrada en**

documentos que registren el ejercicio de las facultades, funciones y competencias de los sujetos obligados, lo que obliga a la autoridad a documentar todo lo relativo a éstas, y presume su existencia, de conformidad con lo establecido en los artículos 3, fracción VII (previamente citado), 4, 18 y 19 de la Ley General[9].

De esta forma, la existencia de la información (y de su presunción) sobre la actividad de una autoridad y la obligación de documentarla, proviene, en todo caso, de que **exista una norma previa que exija la documentación o registro de las actividades que la autoridad realice en ejercicio de sus atribuciones**.

Tal premisa, bajo el diseño contenido en la Ley General de Transparencia, se corrobora con lo dispuesto en su artículo 138, fracción III[10], que para efecto de la generación o reposición de información inexistente, como mecanismo de

---

[9] "**Artículo 3.** Para los efectos de la presente Ley se entenderá por:
[…]
VII. Documento: Los expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas o bien, cualquier otro registro que documente el ejercicio de las facultades, funciones y competencias de los sujetos obligados, sus Servidores Públicos e integrantes, sin importar su fuente o fecha de elaboración. Los documentos podrán estar en cualquier medio, sea escrito, impreso, sonoro, visual, electrónico, informático u holográfico;
Artículo 4. El derecho humano de acceso a la información comprende solicitar, investigar, difundir, buscar y recibir información.
Toda la información generada, obtenida, adquirida, transformada o en posesión de los sujetos obligados es pública y accesible a cualquier persona en los términos y condiciones que se establezcan en la presente Ley, en los tratados internacionales de los que el Estado mexicano sea parte, la Ley Federal, las leyes de las Entidades Federativas y la normatividad aplicable en sus respectivas competencias; sólo podrá ser clasificada excepcionalmente como reservada temporalmente por razones de interés público y seguridad nacional, en los términos dispuestos por esta Ley.
Artículo 18. Los sujetos obligados deberán documentar todo acto que derive del ejercicio de sus facultades, competencias o funciones.
Artículo 19. Se presume que la información debe existir si se refiere a las facultades, competencias y funciones que los ordenamientos jurídicos aplicables otorgan a los sujetos obligados.
En los casos en que ciertas facultades, competencias o funciones no se hayan ejercido, se debe motivar la respuesta en función de las causas que motiven la inexistencia."

[10] **Artículo 138.** Cuando la información no se encuentre en los archivos del sujeto obligado, el Comité de Transparencia:
I. Analizará el caso y tomará las medidas necesarias para localizar la información;
II. Expedirá una resolución que confirme la inexistencia del Documento;
III. Ordenará, siempre que sea materialmente posible, que se genere o se reponga la información en caso de que ésta tuviera que existir en la medida que deriva del ejercicio de sus facultades, competencias o funciones, o que previa acreditación de la imposibilidad de su generación, exponga de forma fundada y motivada, las razones por las cuales en el caso particular no ejerció dichas facultades, competencias o funciones, lo cual notificará al solicitante a través de la Unidad de Transparencia, y
IV. Notificará al órgano interno de control o equivalente del sujeto obligado quien, en su caso, deberá iniciar el procedimiento de responsabilidad administrativa que corresponda.

salvaguarda del derecho de acceso, exige que ésta derive del ejercicio de facultades, competencias o funciones.

El entendimiento de la idea recién anotada constituye el punto de partida para analizar si, en primer lugar, en el espacio de actuación del Máximo Tribunal del país prevalece la condición de que exista una facultad, competencia o función específica respecto de la información materia de la solicitud, para después, en su caso, determinar la eficacia o no del pronunciamiento otorgado al respecto por la instancia involucrada.

En el caso, en relación con los puntos **3, 5, 6** y **13,** la Dirección General de Tecnologías de la Información es competente para pronunciarse sobre estos aspectos de la solicitud, considerando que, en términos del artículo 27 del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación, en específico las fracciones I, II, X y XI[11] en relación con el numeral sexto, fracción VII del Acuerdo General de Administración I/2019, por el que se modifica orgánica y funcionalmente su estructura administrativa, es responsable de administrar los recursos en materia de tecnologías de la información y comunicación, y proveer los servicios que se requieran en la materia, recabar las necesidades de bienes y servicios en materia de tecnologías de la información y comunicación que requieran los órganos y áreas y dictaminar sobre sus características técnicas y sobre la procedencia de incorporarlas en el Programa Anual de Necesidades de Tecnologías de la Información y Comunicación, atender las necesidades tecnológicas en materia de informática jurídica y ejecutar y actualizar los mecanismos de seguridad informática y vigilar su adecuado funcionamiento.

---

[11] **Artículo 27.** El Director General de Tecnologías de la Información tendrá las siguientes atribuciones:
I. Administrar los recursos en materia de tecnologías de la información y comunicación y proveer los servicios que se requieran en la materia;
II. Recabar las necesidades de bienes y servicios en materia de tecnologías de la información y comunicación que requieran los órganos y áreas y dictaminar sobre sus características técnicas y sobre la procedencia de incorporarlas en el Programa Anual de Necesidades de Tecnologías de la Información y Comunicación;
X. Atender las necesidades tecnológicas en materia de informática jurídica;
XI. Ejecutar y actualizar los mecanismos de seguridad informática y vigilar su adecuado funcionamiento…”

Sin embargo, la **Dirección General de Tecnologías de la Información** informa que no cuenta con la información solicitada en los puntos antes referidos y, en algunos casos, están en proceso de planeación y desarrollo los mecanismos de seguridad solicitados.

Por su parte, **la Unidad General de Transparencia** se pronunció respecto la inexistencia de la información solicitada en el punto **7** de la petición en el sentido de que no existe disposición legal que establezca generar un "modelo o sistema de comunicación para informar a los titulares de datos personales en caso de brechas de seguridad".

Asimismo, por lo que hace a si se han adoptado esquemas de mejores prácticas en materia de protección de datos por parte de este Alto Tribunal, como acertadamente lo señala la instancia vinculada, el artículo 72 de la Ley General en cita, establece que el responsable podrá desarrollar o adoptar, en lo individual o en acuerdo con otros responsables, encargados u organizaciones, esquemas de mejores prácticas, lo que significa que dichos esquemas son potestativos de los sujetos obligados; de ahí que también se confirme la inexistencia de la información requerida en el punto **14.**

En similar sentido, en relación con el punto **15,** instancia vinculada señala que no es posible entregar la información requerida, en virtud de que no se ha determinado la existencia de un tratamiento intensivo o relevante de datos personales, en términos de las disposiciones legales de la materia, y por ese motivo se confirma la inexistencia de la información solicitada en este punto.

En este orden de ideas, considerando el pronunciamiento de inexistencia de las instancias referidas y que se exponen las razones por las cuales no se cuenta con la información específica que se pide en la solicitud de acceso, este Comité estima que no se está en el supuesto previsto en la fracción I del artículo 138 de la Ley General de Transparencia[12], conforme al cual deban dictarse otras medidas

[12] "**Artículo 138.** Cuando la información no se encuentre en los archivos del sujeto obligado, el Comité de Transparencia:
I. Analizará el caso y tomará las medidas necesarias para localizar la información;
II. Expedirá una resolución que confirme la inexistencia del Documento;
III. Ordenará, siempre que sea materialmente posible, que se genere o se reponga la información en caso de que ésta tuviera que existir en la medida que deriva del ejercicio de sus facultades, competencias o funciones, o que previa acreditación de la imposibilidad de su

para localizar la información, ya que se trata de las áreas que podrían contar con información de esa naturaleza y han señalado porque no existe la información requerida; además, tampoco se está en el supuesto de exigirles que generen los documentos que se piden conforme lo prevé la fracción III del citado artículo 138 de la Ley General.

En consecuencia, **lo procedente es confirmar la inexistencia de la información analizada en este apartado**, sin que ello constituya una restricción al derecho de acceso a la información dado que se encuentra justificada la imposibilidad de proporcionar lo antes precisado.

Por lo expuesto y fundado, se

R E S U E L V E:

PRIMERO. Se tiene por atendida la solicitud de información en términos del apartado **II.1** de la resolución.

SEGUNDO. Se confirma la inexistencia de la información en términos del apartado **II.2** de la resolución.

TERCERO. Se requiere a la Dirección General de Tecnologías de la Información que atienda las determinaciones de esta resolución.

CUARTO. Se instruye a la Unidad General de Transparencia y Sistematización de la Información Judicial que atienda las determinaciones de esta resolución.

Notifíquese al solicitante, a la instancia requerida, así como a la Unidad General de Transparencia y Sistematización de la Información Judicial de este Alto Tribunal, 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 Maestro Luis Fernando Corona

---

generación, exponga de forma fundada y motivada, las razones por las cuales en el caso particular no ejerció dichas facultades, competencias o funciones, lo cual notificará al solicitante a través de la Unidad de Transparencia, y

IV. Notificará al órgano interno de control o equivalente del sujeto obligado quien, en su caso, deberá iniciar el procedimiento de responsabilidad administrativa que corresponda.”

Horta, Director General de Asuntos Jurídicos y Presidente del Comité; el Maestro Christian Heberto Cymet López Suárez, Contralor del Alto Tribunal; y, el Maestro Julio César Ramírez Carreón, Titular de la Unidad General de Investigación de Responsabilidades Administrativas; integrantes del Comité, ante el Secretario del Comité, que autoriza y da fe.

MAESTRO LUIS FERNANDO CORONA HORTA
PRESIDENTE DEL COMITÉ

MAESTRO CHRISTIAN HEBERTO CYMET LÓPEZ SUÁREZ
INTEGRANTE DEL COMITÉ

MAESTRO JULIO CÉSAR RAMÍREZ CARREÓN
INTEGRANTE DEL COMITÉ

LICENCIADO ARIEL EFRÉN ORTEGA VÁZQUEZ
SECRETARIO 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.