



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

**CUMPLIMIENTO CT-CUM/A-29-2021 derivado del expediente CT-I/A-18-2021**

**INSTANCIA**                      **REQUERIDA:**  
DIRECCIÓN                      GENERAL                      DE  
TECNOLOGÍAS                      DE                      LA  
INFORMACIÓN

Ciudad de México. Resolución del Comité de Transparencia de la Suprema Corte de Justicia de la Nación, correspondiente al **seis de octubre de dos mil veintiuno**.

**ANTECEDENTES:**

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

***“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 ley 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. Resolución del Comité de Transparencia de la Suprema Corte de Justicia de la Nación.** El ocho de septiembre de dos mil veintiuno, este Comité de Transparencia emitió resolución en el expediente CT-I/A-18-2021, en la parte conducente lo siguiente:



*“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.*

*(...)*

**RESUELVE:**

**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...”*

**III. Requerimiento para cumplimiento.** Mediante oficio CT-371-2021, enviado por correo electrónico de trece de septiembre de dos mil veintiuno, la Secretaría de este Comité de Transparencia hizo del conocimiento de la Dirección General de Tecnologías de la Información la resolución antes transcrita, a efecto de que se emitiera el informe requerido.

**IV. Informe del área requerida.** Mediante comunicación electrónica del veintitrés de septiembre de dos mil veintiuno, se remitió a la Secretaría Técnica del Comité de Transparencia el oficio DGTI/409/2021 y la nota de cumplimiento DGTI/DSI/15/2021, en los que se informa:

*“ ... Al respecto, se informa que desde el año 2019 se empezaron a realizar los esfuerzos necesarios para definir la estrategia de ciberseguridad, la cual quedó materializada en el presente año para ser presentada a la Comisión Interna de Protección Civil y de Seguridad, ello en julio de 2021.*

*Se precisa que la estrategia fue creada por la Dirección de Seguridad Informática....”*

**V. Acuerdo de turno.** Mediante acuerdo de veinticuatro de septiembre de dos mil veintiuno, el Presidente del Comité de Transparencia ordenó su remisión a 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 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), así como 23, fracción II, y 27 del Acuerdo General de Administración 5/2015.

### **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 pronunciarse sobre el debido cumplimiento a sus determinaciones; instruir, coordinar y supervisar las acciones y procedimientos para asegurar la eficacia en la gestión de las solicitudes y satisfacer el derecho de acceso a la información, en términos de lo dispuesto en los artículos 6° de la Constitución Política de los Estados Unidos Mexicanos, 4 y 44, fracción I, de la Ley General de Transparencia y Acceso a la Información Pública, así como 23, fracción I, del Acuerdo General de Administración 5/2015.

**II. Análisis.** En la resolución CT-I/A-18-2021, se determinó requerir a la Dirección General de Tecnologías de la Información para que, en relación con lo solicitado por el peticionario en el punto 2 *“Informar si es que se cuenta con una estrategia de ciberseguridad dentro de la institución, en caso de*



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

CUMPLIMIENTO CT-CUM/A-29-2021

*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”, se pronunciara sobre la fecha de creación o implementación de la estrategia de seguridad y las áreas que participaron.*

Al respecto, la Dirección General de Tecnologías de la Información señaló que desde 2019 se iniciaron las actividades para definir la estrategia de ciberseguridad, la cual se materializó el presente año y se presentó en el mes de julio a la Comisión Interna de Protección Civil y de Seguridad. Asimismo, se informa que la estrategia de seguridad fue creada por la Dirección de Seguridad Informática.

Con el informe relatado se atiende lo requerido por este Comité de Transparencia y se satisface el planteamiento del solicitante, toda vez que se precisa el año de creación de la estrategia de seguridad y el área que participó en su creación.

En consecuencia, se solicita a la Unidad General de Transparencia que ponga a disposición de la persona la información proporcionada por el área requerida.

Por lo expuesto y fundado; se,

#### **RESUELVE:**

**PRIMERO.** Se tiene por atendido el requerimiento hecho a la Dirección General de Tecnologías de la Información.

**SEGUNDO.** 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 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 Maestro Luis Fernando Corona 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.