

RESOLUCIÓN DEL COMITÉ PARA LA TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y  
PROTECCIÓN DE DATOS PERSONALES DEL PODER JUDICIAL DEL ESTADO  
DE BAJA CALIFORNIA

NÚMERO DE RESOLUCIÓN: 277/CT/2024  
NÚMERO DE SESIÓN: CT/SE/087/2024  
PROCEDIMIENTO: AMPLIACIÓN DE PLAZO  
FECHA DE LA SESIÓN: 05 DE NOVIEMBRE DE 2024

Mexicali, Baja California. Resolución del Comité para la Transparencia, Acceso a la Información y Protección de Datos Personales del Poder Judicial del Estado de Baja California, correspondiente a la sesión extraordinaria CT/SE/087/2024, celebrada el cinco de noviembre de dos mil veinticuatro.

ANTECEDENTES

1. **Solicitud de acceso a la información pública.** El día veintiuno de octubre de dos mil veinticuatro, en la Plataforma Nacional de Transparencia, se recibió la solicitud de acceso a la información pública 020058424000726, en donde se solicitó conocer lo siguiente:

"PREGUNTAS

APARTADO 1

1. *Informar si dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan;*
2. *Señalar si se cuenta con lo siguiente: a) un marco de mejores prácticas aplicables a la gestión de las TIC en los diferentes procesos de contratación para la adquisición, el arrendamiento de bienes o la prestación de servicios en materia de TIC y de seguridad de la información; Informar si se cuenta con una Inventario Institucional de bienes y servicios de TIC; c) un plan de continuidad de operaciones, y señalar la fecha de implementación; d) Informar si se ha desarrollado e implementado el plan de recuperación ante desastres, señalar la fecha de desarrollo e implementación; e) desarrollado e implementado un programa de gestión de vulnerabilidades; f) Marco de Gestión de Seguridad de la Información (MGSI) o Sistema de Gestión de Seguridad de la Información (SGSI); g) Informar si se cuenta con una política general de seguridad de la información y en su caso, quienes intervienen y desde cuándo se implementó; h) informar si se cuenta con un diagnóstico de identificación de los procesos y activos esenciales de la Institución; i) Informar si se cuenta con un Equipo de Respuesta a Incidentes de Seguridad de la Información (ERISC) o Equipo de respuesta a Incidentes Cibernéticos o en su caso SOC.*



3. *Informar si 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) si es que se ha actualizado o modificado y en cuántas ocasiones; (iv) cuáles áreas participaron en la creación de dicha estrategia ;*
4. *Informar si se emplea la firma electrónica avanzada en la institución;*
5. *Informar si se realizan simulacros sobre el plan de recuperación de desastres o en caso de incidentes cibernéticos;*
6. *Señalar si se cuentan con lineamientos de programación y desarrollo de sistemas informáticos seguros;*
7. *Informar si los servicios de centros de datos son propios, de otra institución gubernamental o de un tercero;*
8. *Informar si para el trabajo remoto se cuentan con lineamientos de seguridad para las videollamadas;*
9. *Informar si se cuenta con un correo electrónico institucional; e Informar si el correo electrónico que se emplea en la institución cuenta con lo siguiente: a) inserción de leyenda de confidencialidad de la información o en su caso de transparencia y acceso a la información; c) control institucional de la totalidad de los correos contenidos en las carpetas de los usuarios; d) Soluciones de filtrado para correo no deseado o correo no solicitado, así como programas informáticos que protejan del envío y recepción de correos electrónicos con software malicioso; e) cuenta con cifrado en el envío de información.*
10. *Informar si se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información Institucional por parte de los servidores públicos;*
11. *Informar si la página web de la institución cuenta con: a) aviso de privacidad; b) certificados digitales vigentes;*
12. *Informar si el personal responsable se ha capacitado en la implementación del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos;*
13. *Informar si se cuentan con: a) Los mecanismos de supervisión y evaluación que permitan medir la efectividad de los controles de seguridad de la*

- información; b) Indicadores que permitan medir el madurez institucional en la gestión de seguridad de la información;
14. Informar si dentro de la institución se cuenta con un Programa de formación en la cultura de la seguridad de la información o de ciberseguridad; y en caso afirmativo señalar: cuándo se implementó.
  15. 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, en caso de ser afirmativa esta pregunta, ¿desde cuándo se adoptó y cuáles áreas participaron en su desarrollo e implementación?;
  16. Informar si 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;
  17. Informar sobre 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;
  18. Informar si se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos;
  19. 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.
  20. Informar si han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas;
  21. Informar si se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son;
  22. 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 de 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; señalar cuáles han sido las recomendaciones vertidas por el del INAI, en su caso;



23. *Informar si se cuenta con documento de seguridad en materia de protección de datos personales;*
24. *Informar si se cuenta con un plan de comunicación institucional en caso de un incidente de ciberseguridad o seguridad de la información;*
25. *Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución;*
26. *Informar si se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad;*
27. *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.*
28. *Señalar si las páginas web de los buscadores de versiones públicas de sentencias del Tribunal, tienen certificados digitales vigentes.*

## APARTADO 2

*Solicito la siguiente información.*

29. *Informar si dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan;*
30. *Informar si 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) si es que se ha actualizado o modificado y en cuántas ocasiones; (iv) cuáles áreas participaron en la creación de dicha estrategia ;*
31. *Informar si se cuenta con un sistema de gestión de seguridad de la información dentro de la institución;*
32. *Informar si 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?;*
33. *Informar si 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;*

34. Informar si 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;

35. Informar sobre 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;

36. Informar si 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;

37. 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;

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

39. 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.

40. Informar si han tenido brechas de ciberseguridad desde el año 2014 a la fecha de la presente solicitud y señalar cuántas;

41. 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;

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

43. 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 de 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; señalar cuáles han sido las recomendaciones vertidas por el del INAI, en su caso;

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

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

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

47. 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.

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

### APARTADO 3

49. Indicar si cuenta con alguna solución tecnológica para juicios en línea, tribunal virtual, e-justice, justicia electrónica, ciberjusticia, ciberseguridad o inteligencia artificial.

50. En caso de contar con alguna solución para el propósito antes señalado, indicar el nombre de la solución tecnológica, dirección de internet donde es accesible, año de inicio de operaciones, materia legal del juicio de la materia de su competencia.

51. En caso de que no cuente con una solución tecnológica para este propósito y tiene conocimiento de alguno en su entidad, favor de indicar el sujeto obligado que pudiera contener dicha información. Me gustaría saber de qué manera aplican medios, instrumentos o aplicaciones que hagan uso de inteligencia artificial dentro del funcionamiento interno de su institución o al momento de brindar servicios a la ciudadanía. En caso de que no, saber si se tienen proyectos para aplicar dicho tipo de tecnología. A su vez se pide conocer lo siguiente:

52. Qué programas, algoritmos, sistemas de inteligencia artificial, sistemas de decisiones judiciales asistidas, algoritmos o programas de selección aleatoria de casos a jueces, tiene y opera.

53. El número de registros existentes de lo solicitado en el punto anterior.

a. Las fechas de operación.

b. El funcionamiento y operación de cada sistema o algoritmo con el que cuenta.

c. Los contratos de su uso o adquisición.

*54.¿Cómo procede y opera la selección y asignación aleatoria de casos a los jueces y juzgados en todas las materias? ¿Cómo se garantiza la independencia judicial a través de estos sistemas de selección y asignación aleatoria de casos?*

*55.¿Qué datos se utilizan para la selección y asignación aleatoria de casos?" (sic)*

2. **Requerimiento de información.** De conformidad con las atribuciones conferidas en el Manual de Organización de la Oficialía Mayor, se identificó que el área competente para generar, obtener, adquirir, transformar o poseer la información solicitada, es el Departamento de Informática.

Por tanto, mediante el oficio 2372/UT/2024 de fecha veintidós de octubre del año dos mil veinticuatro, la Unidad de Transparencia requirió al área para que realizara una búsqueda en sus archivos y en su caso, realice la entrega de la información.

3. **Respuesta al requerimiento.** En fecha cuatro de noviembre de dos mil veinticuatro, se recibió el oficio OM-488/2024, signado por la persona titular de la Oficialía Mayor del Consejo de la Judicatura del Estado, en donde solicitó la ampliación de plazo para dar respuesta, con el objeto de estar en posibilidad de atender la totalidad de los cuestionamientos, de conformidad con lo señalado en el artículo 125 de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Baja California.
4. **Turno al Comité de Transparencia para su análisis.** Una vez integradas las constancias que conforman el expediente, de acuerdo con lo establecido en el artículo 54, fracción II de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Baja California, se procedió a convocar al Comité de Transparencia para analizar el asunto específico a tratar.

## CONSIDERANDOS

5. **Competencia del Comité de Transparencia.** El Comité para la Transparencia, Acceso a la Información y Protección de Datos Personales del Poder Judicial de Baja California, es competente para conocer y resolver el presente asunto, en términos de lo dispuesto en los artículos 6° de la Constitución Política de los Estados Unidos Mexicanos, 44, fracción II de la Ley General de Transparencia y Acceso a la Información Pública, 54, fracción II de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Baja California; 49 y 50 del Reglamento de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Baja California; 11 y 13 del Reglamento para la Transparencia y el Acceso a la Información Pública del Poder Judicial del Estado de Baja California.
6. **Análisis de la solicitud de ampliación de plazo para dar respuesta** En fecha cuatro de noviembre de dos mil veinticuatro, se recibió el oficio OM-488/2024, signado por la persona titular de la Oficialía Mayor del Consejo de la Judicatura del Estado, en donde se solicita la ampliación de plazo para dar respuesta. Esto en razón de que es necesario realizar una búsqueda exhaustiva de la información en los archivos físicos y digitales de esta institución. Con esta ampliación se estaría en posibilidad de realizar un análisis a lo que se solicita y responder cada uno de los cuestionamientos dentro del plazo legal.

Finalmente, este Comité para la Transparencia, Acceso a la Información y Protección de Datos Personales del Poder Judicial del Estado de Baja California, encuentra que las razones y circunstancias que motivan la solicitud de ampliación de plazo, se consideran suficientes, justificadas y fundamentadas para acreditar que se pretende realizar acciones encaminadas a la entrega oportuna de la información objeto de la solicitud, conforme a lo establecido por el artículo 125 de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Baja California.

### RESUELVE

**PRIMERO.** Se **CONFIRMA** la ampliación de plazo para dar respuesta a la solicitud de acceso a la información pública número **020058424000726** por el plazo de diez días hábiles.

**SEGUNDO.** Se instruye a la Unidad de Transparencia para que proceda a publicar la presente resolución en el Portal de Obligaciones de Transparencia de la Plataforma Nacional de Transparencia de conformidad con la fracción XXXIX del artículo 81 de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Baja California.

**TERCERO.** Se instruye a la Unidad de Transparencia para que notifique a la **persona titular de la Oficialía Mayor del Consejo de la Judicatura del Estado**, de acuerdo a lo establecido en los artículos 15, 17 y 26 del Reglamento para la Transparencia y el Acceso a la Información Pública del Poder Judicial del Estado de Baja California.

Así, por unanimidad de votos, lo resolvió el Comité para la Transparencia, Acceso a la Información y Protección de Datos Personales del Poder Judicial del Estado de Baja California y firman el Maestro Alejandro Isaac Fragozo López, Magistrado Presidente del Tribunal Superior de Justicia y del Consejo de la Judicatura en su calidad de Presidente del Comité; la Magistrada Leonor Garza Chávez, la Oficial Mayor del Consejo de la Judicatura Rosaura Zamora Robles, el Director de la Unidad Jurídica y Asesoría Interna del Poder Judicial Santiago Romero Osorio, todos y todas integrantes del Comité, ante la Secretaria Técnica, quien autoriza y da fe.



**MAGISTRADO ALEJANDRO ISAAC FRAGOZO LÓPEZ**  
**PRESIDENTE DEL TRIBUNAL SUPERIOR DE JUSTICIA Y**  
**DEL CONSEJO DE LA JUDICATURA DEL ESTADO**



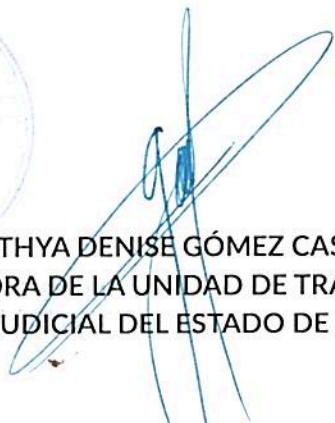
**MAGISTRADA LEONOR GARZA CHÁVEZ**  
ADSCRITA A LA TERCERA SALA COLEGIADA EN MATERIA PENAL DEL  
TRIBUNAL SUPERIOR DE JUSTICIA DEL ESTADO



**C.P. ROSAURA ZAMORA ROBLES**  
OFICIAL MAYOR DEL CONSEJO DE LA JUDICATURA



**LIC. SANTIAGO ROMERO OSORIO**  
DIRECTOR DE LA UNIDAD JURÍDICA Y ASESORÍA INTERNA



**CINTHYA DENISE GÓMEZ CASTAÑEDA**  
DIRECTORA DE LA UNIDAD DE TRANSPARENCIA  
DEL PODER JUDICIAL DEL ESTADO DE BAJA CALIFORNIA

ESTA HOJA DE FIRMAS FORMA PARTE INTEGRAL DE LA RESOLUCIÓN 277/CT/2024, DEL COMITÉ PARA LA TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES DEL PODER JUDICIAL DEL ESTADO DE BAJA CALIFORNIA.

