

OFICIO No. UTEE/1489/2024

AÑO JUDICIAL 2024-2025

ASUNTO: SE REMITE RESPUESTA

Colima; Col. a 06 de noviembre de 2024.

Solicitante: Sin nombre o seudónimo

Contacto: Sistema de solicitudes de la PNT

P r e s e n t e:

De conformidad al artículo 6, apartado A, fracciones I, II y III de la Constitución Política de los Estados Unidos Mexicanos; artículo 5, apartado A y B, fracciones I y II de la Constitución Política del Estado Libre y Soberano de Colima; artículos 1, 4, 11, 12, 13, 15, 16, 17 y 23 de la Ley General de Transparencia y Acceso a la Información Pública; artículos 1, 2, 5, 6, 7, 8, 10, 11, 26 fracción III, 135 y demás aplicables de la Ley de Transparencia y Acceso a la Información Pública del Estado de Colima, artículos 150 fracción VI y 168 de la Ley Orgánica del Poder Judicial del Estado de Colima, así como los artículos 3º, 4º, 5º, 6º y demás aplicables del Reglamento de Transparencia y Acceso a la Pública del Poder Judicial del Estado; en relación a su solicitud de información con número de folio **060111124000166** presentada a través de la Plataforma Nacional de Transparencia a través del SISAI 2.0, y mediante la cual requiere lo siguiente:

Descripción de la solicitud

"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 la 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 se 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 se 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)

Se hace de su conocimiento que su solicitud fue turnada mediante oficio UTEE/1460/2024, a la Dirección de Tecnologías de la Información y Comunicaciones del Supremo Tribunal de Justicia del Estado de Colima, misma que emitió respuesta a la solicitud de información mediante el siguiente oficio número TICS/92/2024 de fecha 31 de octubre de 2024, con el cual se le da respuesta a lo solicitado y se le informa lo siguiente:

APARTADO I

4. Se cuenta con la firma electrónica avanzada FIREL del Poder Judicial de la Federación.
7. Se cuenta con un centro de datos propio y uno más contratado a un tercero como servicio de nube administrada.
9. Si se cuenta con correo electrónico institucional.
 - a) Si cuenta con inserción de leyenda de confidencialidad de la información.
 - c) No hay un control institucional centralizado del contenido de cada cuenta.
 - d) Si cuenta con filtro de spam.



e) Cuenta con cifrado.

11. La página web institucional cuenta con aviso de privacidad y certificados digitales vigentes.

20. No se cuentan con registros de incidencias de ciberseguridad desde el año 2015 a la fecha.

28. Al ser parte de la página web institucional también cuenta con certificados digitales vigentes.

Con respecto a los puntos no mencionados, la respuesta general es que esta institución aún no cuenta con las normativas, herramientas y/o actividades señaladas en cada uno de ellos y/o este órgano administrativo no cuenta con información al respecto.

APARTADO II

40. No se cuentan con registros de incidencias de ciberseguridad desde el año 2014 a la fecha.

Con respecto a los puntos no mencionados, la respuesta general es que esta institución aún no cuenta con las normativas, herramientas y/o actividades señaladas en cada uno de ellos y/o este órgano administrativo no cuenta con información al respecto.

APARTADO III

49. Si se cuenta.

50. Plataforma de Tribunal Electrónico del Poder Judicial del Estado de Colima "eTribunal", únicamente para notificaciones electrónicas y envío de promociones en línea. Se implementó en el segundo trimestre del año 2021.

<https://stjdigitalcolima.gob.mx/#/home>

52. El sistema de oficialía de partes utilizado para el registro y turno de demandas judiciales iniciales hace uso de un algoritmo de turno aleatorio de casos a los juzgados.

53. El algoritmo opera desde hace 15 años aproximadamente y fue un desarrollo interno.

54. El algoritmo toma en cuenta la carga de trabajo de cada juzgado en cada uno de los juicios que por materia conoce cada órgano jurisdiccional, manteniendo un balance en las asignaciones a lo largo del año calendario y al mismo tiempo incorporando una variable de aleatoriedad para que la asignación de un caso sea impredecible. El algoritmo no puede ser modificado sin previa autorización del pleno a través de un acuerdo general y en caso de intentar alguna manipulación quedará registrado en un log que es revisado constantemente.

55. Los datos mínimos requeridos son tipo de juicio y nombre de las partes.

Con respecto a los puntos no mencionados, la respuesta general es que esta institución aún no cuenta con las normativas, herramientas y/o actividades señaladas en cada uno de ellos y/o este órgano administrativo no cuenta con información al respecto.

Ahora bien por lo que respecta a su interrogante **número 2 inciso a) del Apartado 1**, se infoma que este Sueteto Obligado cuenta con un inventario institucional de bienes, el cual puede ser consultado mediante el siguiente enlace:

<https://transparencia.stjcolima.gob.mx/#/declaraciones/34>

Asi mismo, se informa que por lo que corresponde a la **pregunta 31** del Aparatado 2, la Unidad de Transparencia, Evaluación y Estadística este Sujeto Obligado, de confromidad con el artículo 38 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Colima, cuenta con un proyecto de normativa de Seguridad para la Protección de los Datos Personales del Poder Judicial del Estado de Colima, el cual aún se encuentra pendiente para su autorización.

Por lo que corresponde a su **pregunta número 32** del apartado mencionado en el párrafo anterior, se informa en primer lugar que de confimidad con la Leyes



vigentes publicadas por la Camara de Disputados, solo se encuentra publicada la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, la cual NO es competente para el Supremo Tribunal de Justicia del Estado de Colima, esto en virtud dicha ley regula a las personas físicas o morales de carácter privado, lo anterior con fundamento en el artículo 2 de la citada en supralíneas, la cual a la letra dice:

Artículo 2.- *Son sujetos regulados por esta Ley, los particulares sean personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales, con excepción de:*

- I. *Las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables, y*
- II. *Las personas que lleven a cabo la recolección y almacenamiento de datos personales, que sea para uso exclusivamente personal, y sin fines de divulgación o utilización comercial.*

Acerca de la información solicitada en su **interrogante número 39**, se informa que las personas servidoras públicas de la Unidad de Transparencia, Evaluación y Estadística este Sujeto Obligado cuentan con conocimientos en Transparencia, Protección de Datos Personales y Archivos Públicos.

Con respecto a su **pregunta número 42**, se informa durante el año en curso si se han adoptado esquemas de mejores prácticas dentro del Poder Judicial del Estado de Colima, dentro de las cuales fueron:

- La actualización de aviso de privacidad.
- La Capacitación en materia de Protección de Datos Personales y elaboración de sentencias en versión pública para su publicación con personal de la Sala Mixta Civil, Familiar y Mercantil, así como juzgados de lo Familiar del Poder Judicial del Estado de Colima.

Lo anterior de conformidad al artículo 10 de la citada Ley y 6º del Reglamento de Transparencia y Acceso a la Información Pública del Poder Judicial del Estado de Colima, la obligación de proporcionar información no comprende el procesamiento específico de la misma, ni el presentarla conforme al interés del solicitante, sino que deberá ser entregada en el estado en que se encuentre, tampoco comprende la obligación de crear, producir o proporcionar información que no exista o que no se encuentre en posesión del Poder Judicial.

Finalmente, por medio del presente se le hace de su conocimiento que cuenta con un término de 15 días hábiles para presentar el recurso correspondiente, de conformidad con lo establecido en el artículo 151 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Colima.

Esperando que la información proporcionada le sea de utilidad, sin otro en particular, aprovecho la ocasión para enviarle un cordial y respetuoso saludo.

Atentamente

Rúbrica

Licda. Carla Alejandra Martínez Ríos
Encargada de la Unidad de Transparencia
del Poder Judicial del Estado de Colima

