

30 DE OCTUBRE DE 2024
TAIP5-0042-2/2024
UNIDAD DE TRANSPARENCIA

"Sin nombre"
P R E S E N T E.-

En atención a su solicitud de información registrada en el Sistema SISAI- PNT con el número de folio **240477524000042**, recibida en este Tribunal para efectos legales el día tres de septiembre del dos mil veinticuatro, mediante la cual se formulan los siguientes requerimientos de información:

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 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 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.
- Las fechas de operación.
 - El funcionamiento y operación de cada sistema o algoritmo con el que cuenta.
 - 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)

Me permito informarle que esta Unidad de Transparencia en atención a su solicitud de información y de conformidad con el artículo 54 fracciones IV y V de la Ley de Transparencia y Acceso a la Información Pública del Estado de San Luis Potosí, da respuesta a su solicitud en los siguientes términos:

Con fecha veintidós de octubre del dos mil veinticuatro le fue turnada su solicitud de información mediante oficio **N° TAIP5-0042-1/2024** al Ing. Joel Salvador Castañeda López; Titular de la Unidad de Tecnologías de la Información y la Comunicación de este sujeto obligado para la atención de los requerimientos de información que estuvieran dentro de sus facultades y atribuciones para dar respuesta, por lo que con fecha del dieciocho de septiembre del presente año, se recibió respuesta en esta Unidad de Transparencia mediante Oficio **N° UTIC/016/2024** mismo que se adjunta a la presente respuesta, en la cual da respuesta a los requerimientos de información 1, 2 3 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 16, 18, 20, 24, 25, 26, 27, 28, 29, 30, 31, 33, 34, 36, 37, 38, 41, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54 y 55.



Respecto a sus cuestionamientos descritos en los numerales 15, 17, 19, 21, 22, 23, 32, 35, 39, 40, 42 y 43 esta Unidad de Transparencia proporciona las respuestas correspondientes.

Por lo anterior, se adjunta a la presente el listado completo de 55 cuestionamientos en 3 apartados y sus respuestas.

Conforme a lo dispuesto en el artículo 166 de la Ley de Transparencia y Acceso a la Información Pública del Estado de San Luis Potosí; el solicitante podrá interponer, por sí mismo o a través de su representante, de manera directa o por medios electrónicos, recurso de revisión ante la Comisión Estatal de Garantía de Acceso a la Información Pública del Estado de San Luis Potosí o ante la Unidad de Transparencia que haya conocido de la solicitud dentro de los quince días siguientes a la fecha de la notificación de la respuesta, o del vencimiento del plazo su notificación.

A T E N T A M E N T E

**UNIDAD DE TRANSPARENCIA DEL TRIBUNAL
ESTATAL DE JUSTICIA ADMINISTRATIVA
DE SAN LUIS POTOSI**



TRIBUNAL ESTATAL
DE JUSTICIA
ADMINISTRATIVA
San Luis Potosí



TRIBUNAL ESTATAL DE JUSTICIA ADMINISTRATIVA
SAN LUIS POTOSÍ
UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA
COMUNICACIÓN

OFICIO NO. UTIC/016/2024

LIC. ROBERTO TREVIÑO ANDRÉS
TITULAR DE LA UNIDAD DE TRANSPARENCIA, ACCESO
A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE
DATOS PERSONALES.
P R E S E N T E.

Por medio del presente y en atención a su Oficio **TAIP5-0042-1/2024** recibido en esta a mí cargo el veintidós de octubre del presente año, me permito informar lo siguiente:

Con relación a la solicitud de información registrada en el sistema SISAI 2.0 PNT, con el número de folio **240477524000042**, en donde se realizan 55 cuestionamientos en Apartados 1, 2 y 3 le informo que de acuerdo a las funciones y atribuciones de esta Unidad de Tecnologías de la Información y la Comunicación a mi cargo se dio respuesta a los siguientes requerimientos 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 16, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 34, 35, 37, 38, 39, 42, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55:

Por lo anterior, se adjuntan al presente los cuestionamientos y las respuestas.

Aprovecho la ocasión para enviarle un cordial saludo.

San Luis Potosí, el 29 de Octubre de 2024.



UNIDAD DE
JOEL SALVADOR CASTAÑEDA LÓPEZ
TITULAR DE LA UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA
COMUNICACIÓN.

PREGUNTAS

APARTADO 1

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

R.- No se cuenta con un gobierno de seguridad de la información, mas sin embargo se utilizan mecanismos que ayuden en la protección de la información resguardada en el Tribunal.

2. Señalar sí 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 b) sí 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 sí 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 sí se cuenta con una política general de seguridad de la información y en su caso, quienes intervienen y desde cuándo se implementó; h) informar sí se cuenta con un diagnóstico de identificación de los procesos y activos esenciales de la Institución; i) Informar sí 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.

a) Se cuenta con una serie de consideraciones a tener en cuenta al momento de la adquisición de bienes y servicios.

b) Si se cuenta

c) No se cuenta

d) No se ha desarrollado

e) No se ha desarrollado

f) No se cuenta

g) No se cuenta

h) No se cuenta

i) No se cuenta

3. 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 ;

R. No se cuenta con estrategia de ciberseguridad mas sin embargo se tienen considerados aspectos de manera que se minimicen los riesgos a vulnerabilidades.

4. Informar sí se emplea la firma electrónica avanzada en la institución;

R. No se emplea la firma electrónica avanzada

5. Informar si se realizan simulacros sobre el plan de recuperación de desastres o en caso de incidentes cibernéticos;
R. No se realizan
6. Señalar si se cuentan con lineamientos de programación y desarrollo de sistemas informáticos seguros;
R. No se cuenta, mas sin embargo se utiliza la metodología SCRUM
7. Informar si los servicios de centros de datos son propios, de otra institución gubernamental o de un tercero;
R. Se cuentan con centros de datos tanto propios como de terceros.
8. Informar si para el trabajo remoto se cuentan con lineamientos de seguridad para las video llamadas;
R. No se cuentan
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.
R. Si se cuenta con correo institucional
 - a) No se cuenta
 - c) Directo con el proveedor
 - d) Directo con el proveedor
10. Informar si se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información Institucional por parte de los servidores públicos;
R. La divulgación no autorizada de la información sustantiva de este sujeto obligado cuenta con restricciones legales previstas en diversa normatividad como lo es el Código Procesal Administrativo, La Ley de Transparencia y Acceso a la Información Pública de San Luis Potosí respecto a aquella información de procedimientos seguidos en forma de juicios en tanto no se dicte sentencia cause estado y ejecutoria, La Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados que prohíbe la difusión de los datos personales la vulneración al uso de la información puede ser motivo de procedimiento de responsabilidad administrativa mecanismo que inhibe la divulgación de la información no autorizada.
11. Informar si la página web de la institución cuenta con: a) aviso de privacidad; b) certificados digitales vigentes;
R. Si se cuenta con avisos de privacidad en la sección de transparencia y cuenta con sus certificados SSL vigentes
12. Informar si el personal responsable se ha capacitado en la implementación del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos;
R. El personal ha asistido a cursos y conferencias en temas de Ciberseguridad

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;

R. No se cuenta

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.

R. No se cuenta, más sin embargo se imparten recomendaciones para mitigar riesgos de pérdida de información

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?;

R. Está en etapa de desarrollo el sistema de gestión de protección de datos personales el cual involucra a todas las áreas de este sujeto obligado y en tanto no esté terminado y autorizado por el Comité de Transparencia no se puede difundir información al respecto.

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;

R. No se cuenta

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;

R=No se cuenta con un modelo o sistema de comunicación, ya que se procedería conforme a lo establecido en el artículo 56 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de San Luis Potosí que señala:

ARTÍCULO 56. El responsable deberá informar sin dilación alguna al titular y a la CEGAIP las vulneraciones de seguridad ocurridas, que de forma significativa afecten los derechos patrimoniales o morales del titular, en un plazo máximo de setenta y dos horas en cuanto se confirmen, y 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.

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

R. No se cuenta

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.
R. Si cuentan con experiencia comprobable en dichos temas.
20. Informar si han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas;
R. No se han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la solicitud de información.
21. Informar si se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son;
R. En la elaboración de Versiones Publicas se adoptó un sistema interno para proteger los datos personales así como se fomentó el uso del TEST DATA avalado por el Sistema Nacional de Transparencia.
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;
R. En la elaboración de Versiones Publicas de las Sentencias y no se han realizado recomendaciones por parte del INAI.
23. Informas si se cuenta con documento de seguridad en materia de protección de datos personales;
R. Está en etapa de desarrollo el sistema de gestión de protección de datos personales y el documento de seguridad, el cual involucra a todas las áreas de este sujeto obligado y en tanto no esté terminado y autorizado por el Comité de Transparencia no se puede difundir información al respecto.
24. Informar si se cuenta con un plan de comunicación institucional en caso de un incidente de ciberseguridad o seguridad de la información;
R. No se cuenta
25. Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución;
R. Diariamente la Unidad de Tecnologías de la Información se mantiene actualizada ante posibles vulnerabilidades cibernéticas
26. Informar si se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad;
R. No se realizan
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.
R. No se cuenta, mas sin embargo se atienden de manera oportuna cualquier incidencia

28. Señalar si las páginas web de los buscadores de versiones públicas de sentencias del Tribunal, tienen certificados digitales vigentes.

R. Si cuentan con 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;

R.- No se cuenta con un gobierno de seguridad de la información, mas sin embargo se utilizan mecanismos que ayuden en la protección de la información resguardada en el Tribunal.

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 ;

R. No se cuenta con estrategia de ciberseguridad mas sin embargo se tienen considerados aspectos de manera que se minimicen los riesgos a vulnerabilidades.

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

R. Está en etapa de desarrollo el sistema de gestión de protección de datos personales y el documento de seguridad, el cual involucra a todas las áreas de este sujeto obligado y en tanto no esté terminado y autorizado por el Comité de Transparencia no se puede difundir información al respecto.

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?;

R. Está en etapa de desarrollo el sistema de gestión de protección de datos personales y el documento de seguridad, el cual involucra a todas las áreas de este sujeto obligado y en tanto no esté terminado y autorizado por el Comité de Transparencia no se puede difundir información al respecto.

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;

R. No se cuenta

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;

R. No se cuenta

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;

R. No se cuenta con un modelo o sistema de comunicación, ya que se procedería conforme a lo establecido en el artículo 56 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de San Luis Potosí que señala:

ARTÍCULO 56. El responsable deberá informar sin dilación alguna al titular y a la CEGAIP las vulneraciones de seguridad ocurridas, que de forma significativa afecten los derechos patrimoniales o morales del titular, en un plazo máximo de setenta y dos horas en cuanto se confirmen, y 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.

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;

R. No se cuenta, más sin embargo se imparten recomendaciones para mitigar riesgos de pérdida de información

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;

R. No se cuenta

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

R. No se cuenta

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.

R. Si cuentan con experiencia comprobable en dichos temas.

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

R. No se han tenido brechas de ciberseguridad desde el año 2014 a la fecha de la solicitud de información.

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;

R. No se cuenta

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

R. En la elaboración de Versiones Publicas se adoptó un sistema interno para proteger los datos personales así como se fomentó el uso del TEST DATA avalado por el Sistema Nacional de Transparencia.

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 INAI, en su caso;

R. En la elaboración de Versiones Publicas de las Sentencias y no se han realizado recomendaciones por parte del INAI.

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

R. Diariamente la Unidad de Tecnologías de la Información se mantiene actualizada ante posibles vulnerabilidades cibernéticas

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

R. No se realizan

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

R. No se cuenta, mas sin embargo se atienden de manera oportuna cualquier incidencia

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.

R. No se cuenta, mas sin embargo se atienden de manera oportuna cualquier incidencia

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

R. No se cuenta

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.

R. No se cuenta

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.

R. No se cuenta

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:

R. No se tiene conocimiento

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.

R. No se tiene conocimiento

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.

R. No se tiene conocimiento

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?

R. Se diseñó un algoritmo el cual en base a los asuntos ya turnados clasificados en fondo y forma de cada sala asigna las demandas ingresadas

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

R. El número de asuntos de cada sala clasificados en fondo y forma