Tlaxcala, Tlaxcala, a 13 de noviembre de 2024
Asunto: Respuesta a solicitud de información pública.

nacidoel1deenero@gmail.com
P R E S E N T E

En atención a su solicitud de ejercicio de información de fecha veintidós de octubre de dos mil veinticuatro, recibida en la Unidad de Transparencia del Tribunal de Conciliación y Arbitraje del Estado de Tlaxcala 290538824000039, mediante la cual solicita la siguiente información:

"Descripción de la solicitud:
Archivo adjunto.

Se da respuesta en los siguientes términos:

Con fundamento en los artículos 116, 118, y 121 de la ley de Transparencia y Acceso a la Información Pública del Estado de Tlaxcala, se da contestación a la solicitud de información.

De acuerdo con lo especificado en su solicitud de información remitida a este Tribunal de Conciliación y Arbitraje del Estado de Tlaxcala, le informamos que las respuestas a sus interrogantes se encuentran a continuación en el documento denominado Anexo 1, mismo que consta de 8 hojas, desagregadas y contestadas en el mismo orden en el que fueron solicitadas.

Sin más por el momento, le envío un cordial saludo.

A T E N T A M E N T E

KAREN BELEM RAMÍREZ AVILA
TITULAR DE LA UNIDAD DE TRANSPARENCIA DEL
TRIBUNAL DE CONCILIACIÓN Y ARBITRAJE DEL ESTADO DE TLAXCALA

Calle Guerrero No. 27 Col. Centro Tlaxcala, Tlax. C.P. 90000 Teléfonos: 01 246 46 266 70 y 46 2 74 10
Correo Electrónico: tricyatx@tca-tlax.org

Anexo 1

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

   - No se cuenta con un gobierno de seguridad de la información ni con un área dedicada a la ciberseguridad.

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:**

   - No se dispone de un marco formal de mejores prácticas en la gestión de TIC para procesos de contratación.

b) **Inventario Institucional de bienes y servicios de TIC:**

   - Se cuenta únicamente con un inventario general de bienes muebles, sin un inventario específico de bienes y servicios de TIC.

c) **Plan de continuidad de operaciones, y señalar la fecha de implementación:**

   - No se cuenta con un plan de continuidad de operaciones.

d) **Plan de recuperación ante desastres, y señalar la fecha de desarrollo e implementación:**

   - No se dispone de un plan de recuperación ante desastres.

e) **Programa de gestión de vulnerabilidades:**

   - No se cuenta con 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):**

   - No se dispone de un MGSI ni de un SGSI.

g) **Política general de seguridad de la información, quiénes intervienen y desde cuándo se implementó:**

   - No se cuenta con una política general de seguridad de la información.

h) **Diagnóstico de identificación de los procesos y activos esenciales de la Institución:**

   - No se cuenta con un diagnóstico de procesos y activos esenciales.

i) **Equipo de Respuesta a Incidentes de Seguridad de la Información (ERISC) o Equipo de Respuesta a Incidentes Cibernéticos o en su caso SOC:**

   - No se dispone de un ERISC ni de un SOC.

3. **Informar si se cuenta con una estrategia de ciberseguridad dentro de la institución, y en caso afirmativo, informar lo siguiente:**

- No se cuenta con una estrategia formal de ciberseguridad.

4. **Informar si se emplea la firma electrónica avanzada en la institución:**
   - 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:**
   - No se realizan simulacros de este tipo.
6. **Señalar si se cuentan con lineamientos de programación y desarrollo de sistemas informáticos seguros:**
   - No se cuenta con lineamientos para programación y desarrollo seguro de sistemas informáticos.
7. **Informar si los servicios de centros de datos son propios, de otra institución gubernamental o de un tercero:**
   - Los servicios de tecnología se adquieren a través de proveedores externos.
8. **Informar si para el trabajo remoto se cuentan con lineamientos de seguridad para las videollamadas:**
   - No se cuenta con lineamientos de seguridad para videollamadas en trabajo remoto.
9. **Informar si se cuenta con un correo electrónico institucional y si este incluye inserción de leyenda de confidencialidad, control institucional, filtrado de spam, y cifrado:**
   - El correo electrónico institucional cuenta únicamente con las funciones de seguridad proporcionadas por el proveedor, como el filtrado de spam. No se tiene configurada la inserción de una leyenda de confidencialidad.
10. **Informar si se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información Institucional por parte de los servidores públicos:**
    - No se cuenta con mecanismos formalizados para prevenir la divulgación no autorizada de datos. No obstante, los servidores públicos están sujetos a la Ley de Responsabilidades de los Servidores Públicos para el Estado de Tlaxcala, la cual establece obligaciones y sanciones aplicables a quienes incurran en actos u omisiones que puedan afectar el desempeño de sus funciones o los intereses públicos. Esta ley incluye disposiciones sobre la responsabilidad administrativa y posibles sanciones en casos de uso indebido de la información o cualquier acción que perjudique a la institución.
11. **Informar si la página web de la institución cuenta con aviso de privacidad y certificados digitales vigentes:**
    - Si cuenta con cuenta con aviso de privacidad y certificados digitales vigentes

Anexo 1

12. **Informar si el personal responsable se ha capacitado en el Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos:**

    - No se han realizado capacitaciones en dicho protocolo.

13. **Informar si se cuentan con mecanismos de supervisión y evaluación para medir la efectividad de los controles de seguridad de la información, así como indicadores de madurez en seguridad:**

    - No se cuenta con mecanismos de supervisión, evaluación o indicadores de madurez en seguridad de la información.

14. **Informar si 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:**

    - No se cuenta con un programa de formación en seguridad de la información o ciberseguridad.

15. **Informar si se cuenta con un sistema de gestión de protección de datos personales conforme a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados:**

    - Actualmente, no se cuenta con un sistema integral de gestión de protección de datos personales conforme a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Sin embargo, se implementan procedimientos relacionados, tales como la designación de un Oficial de Protección de Datos Personales y la gestión de solicitudes de derechos ARCO, además de capacitar al personal en materia de protección de datos personales, todo con el objetivo de cumplir en la mayor medida posible con la normativa aplicable y proteger adecuadamente los datos personales que resguarda este tribunal.

16. **Informar si se cuenta con un modelo o sistema de comunicación para informar a la sociedad sobre eventos de seguridad de la institución, y en caso afirmativo, cuáles áreas participan y desde cuándo se implementó:**

    - No se cuenta con un modelo o sistema de comunicación para informar a la sociedad en caso de incidentes de seguridad.

17. **Informar si se cuenta con un modelo o sistema de comunicación para informar a titulares de datos personales en caso de brechas de seguridad, señalando las áreas participantes y la fecha de implementación:**

    - No se cuenta con un sistema específico para notificar a titulares de datos personales en caso de brechas de seguridad.

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

    - No existen lineamientos específicos para el traslado de activos físicos.

Anexo 1

19. **Informar si el personal encargado de sistemas de información cuenta con conocimientos comprobables en transparencia, protección de datos personales, archivos públicos o seguridad de la información:**

    - El personal encargado de sistemas de información ha recibido capacitaciones en transparencia, protección de datos personales, así como en gestión documental y archivística. No obstante, no se dispone de evidencia comprobable de conocimientos en seguridad de la información.

20. **Informar si han tenido brechas de ciberseguridad desde el año 2014 a la fecha y cuántas:**

    - No se cuenta con un registro específico de brechas de ciberseguridad.

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

    - No se cuenta con un modelo de madurez en seguridad de la información o ciberseguridad.

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

    - Sí, se han adoptado algunos esquemas de mejores prácticas en materia de protección de datos personales. Estos incluyen la implementación de avisos de privacidad, la designación de un Oficial de Protección de Datos Personales, y la gestión de solicitudes de derechos ARCO, entre otros procedimientos que contribuyen al cumplimiento de la normativa en protección de datos.

23. **Informar si algún sistema o plataforma implica el tratamiento intensivo de datos personales, y si se han hecho evaluaciones de impacto, señalando recomendaciones del INAI si existen:**

    - No existen plataformas tecnológicas intensivas en el tratamiento de datos personales ni se han realizado evaluaciones de impacto.

24. **Informar si se cuenta con un documento de seguridad en materia de protección de datos personales:**

    - No se cuenta con un documento formal de seguridad en protección de datos personales.

25. **Informar si se cuenta con un plan de comunicación en caso de un incidente de ciberseguridad o seguridad de la información:**

    - No se cuenta con un plan de comunicación para incidentes de ciberseguridad o seguridad de la información.

26. **Informar cada cuánto tiempo se actualizan las medidas de ciberseguridad dentro de la institución:**

- Como medida de ciberseguridad, se cuenta con el uso de un software antivirus, el cual se actualiza bajo demanda. No se realizan otras actualizaciones adicionales de medidas de ciberseguridad.

27. **Informar si se llevan auditorías de seguridad externas o internas en ciberseguridad, y su periodicidad:**

    - No se realizan auditorías de seguridad en ciberseguridad, ni externas ni internas.

28. **Señalar si se cuenta con un help desk para incidencias reportadas por los servidores públicos, y si es interno o externo:**

    - No se cuenta con un sistema help desk formal para gestionar incidencias.

29. **Informar si se cuenta con una solución tecnológica para juicios en línea, tribunal virtual, e-justice, justicia electrónica, ciberjusticia, ciberseguridad o inteligencia artificial:**

    - No se cuenta con soluciones tecnológicas en estas áreas Se dispone de un sistema de gestión documental propio, y recientemente se firmó un convenio con el Supremo Tribunal de Jalisco para implementar el software "Elida" para generar versiones públicas de sentencias.

30. **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:**

    - La solución es el software "Elida," del Supremo Tribunal de Jalisco. Aún no se ha implementado, por lo que no cuenta con una dirección de internet ni con fecha de inicio de operaciones.

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

    - No se cuenta con un sistema de gestión de seguridad de la información.

32. **Informar si se cuenta con un sistema de gestión de protección de datos personales conforme a la Ley General de Protección de Datos Personales en Posesión de Particulares:**

    - No se cuenta con un sistema formal de gestión de protección de datos personales.

33. **Informar si 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:**

    - No se cuenta con un plan de continuidad del negocio para eventos de seguridad cibernética o física.

34. **Informar si se cuenta con un modelo o sistema de comunicación para informar a la sociedad sobre eventos de seguridad de la institución, y en caso afirmativo, cuáles áreas participan y desde cuándo se implementó:**

- No se cuenta con un modelo o sistema de comunicación para informar a la sociedad en caso de incidentes de seguridad.

35. **Informar si se cuenta con un modelo o sistema de comunicación para informar a titulares de datos personales en caso de brechas de seguridad, señalando las áreas participantes y la fecha de implementación:**

    - No se cuenta con un sistema específico para notificar a titulares de datos personales en caso de brechas de seguridad.

36. **Informar si se realiza capacitación continua a los servidores públicos en materia de ciberseguridad, con qué frecuencia y los temas abordados:**

    - No se realizan capacitaciones continuas en ciberseguridad.

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:**

    - No se cuenta con un procedimiento específico para detección y respuesta ante amenazas.

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

    - No existen lineamientos específicos para el traslado de activos físicos.

39. **Informar si el personal encargado de sistemas de información cuenta con conocimientos comprobables en transparencia, protección de datos personales, archivos públicos o seguridad de la información:**

    - El personal encargado de sistemas de información ha recibido capacitaciones en transparencia, protección de datos personales, así como en gestión documental y archivística. No obstante, no se dispone de evidencia comprobable de conocimientos en seguridad de la información.

40. **Informar si han tenido brechas de ciberseguridad desde el año 2014 a la fecha y cuántas:**

    - No se cuenta con un registro específico de brechas de ciberseguridad.

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

    - No se cuenta con un modelo de madurez en seguridad de la información o ciberseguridad.

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

    - No se han adoptado esquemas formales de mejores prácticas en protección de datos personales.

43. **Informar si algún sistema o plataforma implica el tratamiento intensivo de datos personales, y si se han hecho evaluaciones de impacto, señalando recomendaciones del INAI si existen:**

    - No existen plataformas intensivas en el tratamiento de datos personales ni se han realizado evaluaciones de impacto.

44. **Informar cada cuánto tiempo se actualizan las medidas de ciberseguridad dentro de la institución:**

    - Como medida de ciberseguridad, se cuenta con el uso de un software antivirus, el cual se actualiza bajo demanda. No se realizan otras actualizaciones adicionales de medidas de ciberseguridad.

45. **Informar si se llevan auditorías de seguridad externas o internas en ciberseguridad, y su periodicidad:**

    - No se realizan auditorías de seguridad en ciberseguridad, ni externas ni internas.

46. **Señalar si se cuenta con un sistema de gestión de incidentes y cuáles áreas participan:**

    - No se cuenta con un sistema de gestión de incidentes.

47. **Señalar si se cuenta con un help desk para incidencias reportadas por los servidores públicos, y si es interno o externo:**

    - No se cuenta con un sistema help desk para incidencias.

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

    - No se cuenta con un equipo de respuesta a incidentes cibernéticos.

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

    - No se cuenta con soluciones tecnológicas en estas áreas. Se dispone de un sistema de gestión documental propio, y recientemente se firmó un convenio con el Supremo Tribunal de Jalisco para implementar el software "Elida" para generar versiones públicas de sentencias.

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:**

    - La solución es el software "Elida," del Supremo Tribunal de Jalisco. Aún no se ha implementado, por lo que no cuenta con una dirección de internet ni fecha de inicio de operaciones.

51. **En caso de que no cuente con una solución tecnológica para este propósito y tiene conocimiento de alguno en su entidad, indicar el sujeto obligado que pudiera contener dicha información. También, de qué manera se aplican medios, instrumentos o**

aplicaciones que hagan uso de inteligencia artificial dentro del funcionamiento interno de su institución o al brindar servicios a la ciudadanía. Indicar si hay proyectos para aplicar este tipo de tecnología:

- No se cuenta con una solución de este tipo ni con proyectos que involucren inteligencia artificial en los procesos internos o en servicios a la ciudadanía. La colaboración reciente con el Supremo Tribunal de Jalisco facilitará el uso del software "Elida" para la generación de versiones públicas de sentencias.

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:**

- No se cuenta con programas, algoritmos o sistemas de inteligencia artificial, ni con sistemas de decisiones judiciales asistidas o de selección aleatoria de casos.

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, y los contratos de su uso o adquisición:**

- No aplica, ya que no se cuenta con los sistemas o algoritmos mencionados.

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?**

- No se cuenta con un sistema de selección y asignación aleatoria de casos a jueces.

55. **Qué datos se utilizan para la selección y asignación aleatoria de casos:**

- No aplica, ya que no se cuenta con un sistema de selección y asignación aleatoria de casos.