**COORDINACIÓN DE TRANSPARENCIA.**
**UNIDAD DE TRANSPARENCIA.**
**Oficio: TEJABC/CT/255/2024**
**Asunto: Entrega de Información 020068124000083.**

Mexicali, Baja California, a 15 de noviembre de 2024.

**SOLICITUD CON NÚMERO DE FOLIO: 020068124000083**
En atención a su solicitud de información, se hace de su conocimiento lo siguiente:

**Información requerida:**

*"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;*
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 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.*
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 ;*
4. *Informar sí se emplea la firma electrónica avanzada en la institución;*
5. *Informar sí 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 sí los servicios de centros de datos son propios, de otra*

*institución gubernamental o de un tercero;*

8. *Informar sí para el trabajo remoto se cuentan con lineamientos de seguridad para las videollamadas;*
9. *Informar sí 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 sí se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información Institucional por parte de los servidores públicos;*
11. *Informar sí la página web de la institución cuenta con: a) aviso de privacidad; b) certificados digitales vigentes;*
12. *Informar sí 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 sí 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 sí 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 sí se cuenta con un modelo o sistema de comunicación, para informar a la sociedad en general sobre los eventos o incidentes de seguridad de la institución, y en caso de ser afirmativo, ¿cuáles áreas de la institución que participan? e informar desde cuándo se implementó;*
17. *Informar sobre sí se cuenta con un modelo o sistema de comunicación para informar a los titulares de datos personales en caso de brechas de seguridad de esta información, y señalar cuáles áreas de la organización participan en su implementación y desde cuándo se implementó;*
18. *Informar sí se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos;*
19. *Informar sí las personas encargadas de sistemas de información, donde se brinde información pública, cuentan con conocimientos comprobables en las siguientes materias (i) transparencia; (ii)*

*protección de datos personales; (iii) archivos públicos; o, (iv) seguridad de la información.*

20. *Informar sí han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas;*
21. *Informar sí se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son;*
22. *Informar sí algún sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que se emplee implica el tratamiento intensivo y/o relevante de datos personales, de conformidad de la Ley en la materia; en caso afirmativo señalar sí se han llevado a cabo evaluaciones de impacto en materia de protección de datos personales; señalar cuáles han sido las recomendaciones vertidas por el del INAI, en su caso;*
23. *Informas sí se cuenta con documento de seguridad en materia de protección de datos personales;*
24. *Informar sí 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 sí 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 sí 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 sí dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan;*
30. *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 ;*
31. *Informar sí se cuenta con un sistema de gestión de seguridad de la información dentro de la institución;*
32. *Informar sí de conformidad con la Ley General de Protección de Datos Personales en Posesión de Particulares se cuenta con lo siguiente Un sistema de gestión de protección de datos personales, en caso de ser afirmativa esta pregunta, ¿desde cuándo se adoptó y cuáles áreas participaron en su desarrollo e implementación?;*
33. *Informar sí es que se cuenta con un plan de continuidad del negocio, para el caso de algún evento o incidente de seguridad cibernética o*

*física e informar desde cuándo se implementó;*

34. *Informar sí se cuenta con un modelo o sistema de comunicación, para informar a la sociedad en general sobre los eventos o incidentes de seguridad de la institución, y en caso de ser afirmativo, ¿cuáles áreas de la institución que participan? e informar desde cuándo se implementó;*
35. *Informar sobre sí se cuenta con un modelo o sistema de comunicación para informar a los titulares de datos personales en caso de brechas de seguridad de esta información, y señalar cuáles áreas de la organización participan en su implementación y desde cuándo se implementó;*
36. *Informar sí se realiza capacitación continua a los servidores públicos en materia de ciberseguridad y cada cuándo se lleva a cabo, así como los temas que se abordan;*
37. *Informar sí se cuenta con un procedimiento en caso de detección de alguna amenaza o vulneración de seguridad y cuál es el área encargada de atender los reportes;*
38. *Informar sí se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos;*
39. *Informar sí las personas encargadas de sistemas de información, donde se brinde información pública, cuentan con conocimientos comprobables en las siguientes materias (i) transparencia; (ii) protección de datos personales; (iii) archivos públicos; o, (iv) seguridad de la información.*
40. *Informar sí han tenido brechas de ciberseguridad desde el año 2014 a la fecha de la presente solicitud y señalar cuántas;*
41. *Informar sí se cuenta con un modelo de madurez de seguridad de la información o ciberseguridad dentro de la institución, en caso afirmativo informar desde cuándo se implementa;*
42. *Informar sí se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son;*
43. *Informar sí algún sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que se emplee implica el tratamiento intensivo y/o relevante de datos personales, de conformidad de la ey en la materia; en caso afirmativo señalar sí se han llevado a cabo evaluaciones de impacto en materia de protección de datos personales; señalar cuáles han sido las recomendaciones vertidas por el del INAI, en su caso;*
44. *Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución;*
45. *Informar sí 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 se selección y asignación aleatoria de casos?*
55. *¿Qué datos se utilizan para la selección y asignación aleatoria de casos?." (sic)*

Con apoyo en lo previsto por el artículo 56, fracción II, de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Baja California, **se admite** la solicitud presentada, tomando en cuenta que reúne los requisitos establecidos en el artículo 117 de la Ley en cita.

**Área (s) a la (s) que se turnó:**

1. Coordinadora de Sistemas Informáticos.
2. Unidad de Transparencia.

**Respuesta:**

En cumplimiento a lo establecido en el artículo 56, fracción V, de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Baja California, comuníquese al solicitante, en vía de respuesta lo siguiente:

Se informa al solicitante que esta **Unidad de Transparencia resultó competente** para atender los requerimientos señalados con los numerales **10, 15, 16, 17, 21, 22, 23, 32, 34, 35, 42 y 43.** Respecto de los restantes, se remite al solicitante el oficio de respuesta del área competente.

**RESPUESTAS DE LA UNIDAD DE TRANSPARENCIA:**

10. Informar sí se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información Institucional por parte de los servidores públicos:
**Respuesta: Respecto al presente cuestionamiento se informa que, para evitar la divulgación no autorizada de datos personales o información confidencial por parte de los servidores públicos, este Tribunal estableció los siguientes mecanismos:**

a. **Dentro del primer acuerdo de dictado por los órganos de primera instancia (Juzgados y Sala Especializada en Materia de Responsabilidades Administrativas y Combate a la Corrupción) en cada expediente se debe colocar un apartado denominado "Transparencia", en donde se hace del conocimiento de las partes lo siguiente:**

   ***"Se hace del conocimiento de las partes que la sentencia que se dicte en el presente asunto, estará a disposición del público para su consulta en versión pública dentro del portal de internet del Tribunal, una vez que haya sido notificada, por lo que no incluirá sus datos personales manteniendo el carácter de información confidencial. Asimismo, se les informa que pueden otorgar su consentimiento respecto a la publicación de sus datos personales de manera expresa. Lo anterior en cumplimiento a las obligaciones en materia de transparencia y protección de datos personales contenidas en los artículos 6, 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 106 y 116 de la Ley General de Transparencia y Acceso a la Información Pública; 4, fracciones VI, XII y XXVI, 80, 83, fracción VI, inciso b) y 106 de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Baja California; 171, párrafo primero y 172 del Reglamento de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Baja California; así como, lo previsto en los artículos 9 y 10 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Baja California."***

b. **El personal de oficialía de partes (recepción) de cada una de las oficinas del Tribuna tiene instrucciones de no proporcionar información sobre ningún asunto sin corroborar mediante identificación oficial que se encuentran autorizados o son parte del juicio.**

c. **Dentro del Portal Web del Tribunal, existe un apartado denominado "Avisos de Privacidad", el cual contiene todos los avisos de privacidad de los diversos tratamientos de datos personales que realiza el Tribunal y es de conocimiento de todos los servidores públicos y la ciudadanía.**

d. **En el año 2021, se aprobó por el Pleno de este Tribunal el "Catálogo de Datos Personales, Criterios y Resoluciones para su Tratamiento", así como los "Lineamientos para la Elaboración de Versiones Públicas del Tribunal Estatal de Justicia Administrativa de Baja California", documentos encaminados a la protección de los datos personales tratados por este Tribunal, los cuales son de conocimiento de todos los servidores públicos y la ciudadanía.**

15. Informar sí 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?:
**Respuesta: Respecto a este punto se informa que a la fecha el Sistema de Gestión se encuentra en proceso de desarrollo con la participación de todas las áreas necesarias para cada etapa; cabe señalar que como parte del Sistema de Gestión, de conformidad con el artículo 18 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Baja California, *"El responsable debe elaborar un documento de seguridad y actualizarlo conforme a los supuestos que enmarca la Ley General"*, mientras que el artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados establece los documentos que integran el Documento de Seguridad, consistentes en:**

*I. El inventario de datos personales y de los sistemas de tratamiento;*
*II. Las funciones y obligaciones de las personas que traten datos personales;*
*III. El análisis de riesgos;*
*IV. El análisis de brecha;*
*V. El plan de trabajo;*
*VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y*
*VII. El programa general de capacitación.*

**Con base en lo anterior, se informa que este Tribunal cuenta con:**

| Documento | Estado |
|---|---|
| 1. *El inventario de datos personales y de los sistemas de tratamiento;* | Proyecto en revisión |
| 3. *Las funciones y obligaciones de las personas que traten datos personales;* | Proyecto en revisión |
| 4. *El análisis de riesgos;* | Pendiente |
| 5. *El análisis de brecha;* | Pendiente |

| | |
|---|---|
| 6. *El plan de trabajo;* | **Pendiente** |
| 7. *Los mecanismos de monitoreo y revisión de las medidas de seguridad, y* | **Pendiente, debido a que resultarán de las conclusiones del análisis de riesgos.** |
| 8. *El programa general de capacitación.* | **Proyecto 2025 en revisión** |

16. Informar sí se cuenta con un modelo o sistema de comunicación, para informar a la sociedad en general sobre los eventos o incidentes de seguridad de la institución, y en caso de ser afirmativo, ¿cuáles áreas de la institución que participan? e informar desde cuándo se implementó.
**Respuesta: Por el momento no se cuenta con un modelo o sistema de comunicación.**

17. Informar sobre sí se cuenta con un modelo o sistema de comunicación para informar a los titulares de datos personales en caso de brechas de seguridad de esta información, y señalar cuáles áreas de la organización participan en su implementación y desde cuándo se implementó:
**Respuesta: Por el momento no se cuenta con un modelo o sistema de comunicación.**

21. Informar sí se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son:
**Respuesta: Si; recientemente se ha incluido dentro del Portal Web del Tribunal, la siguiente página: https://tejabc.mx/solicitudesarco , en la cual de manera sencilla y amigable se pone a disposición de la ciudadanía los formatos que les permitirán ejercer sus derechos ARCO, presentar denuncias y recursos de revisión en esta materia. Asimismo, existe el apartado https://tejabc.mx/derechos-arco , mediante el cual se informa todo lo relacionado con el ejercicio de derechos ARCO, conceptos, requisitos, formatos, plazos, notificaciones, requisitos específicos, etc. Con estas dos herramientas digitales se facilita el ejercicio de derechos ARCO por parte de los titulares.**
**Por otra parte, en fecha 7 de noviembre de 2024, el Pleno de este Tribunal aprobó el Nuevo Catálogo de Protección de Datos Personales, criterios y resoluciones para su tratamiento (versión 2024), con lo cual se eleva el nivel de protección de los datos personales pues los servidores públicos de este Tribunal pueden acudir a dicho documento para resolver dudas sobre toda aquella información que pudiera revestir la calidad de confidencial.**

22. Informar sí algún sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que se emplee implica el tratamiento intensivo y/o relevante de datos personales, de conformidad de la Ley en la materia; en caso afirmativo señalar sí se han llevado a cabo evaluaciones de impacto en materia de protección de datos personales; señalar cuáles han sido las recomendaciones vertidas por el del INAI, en su caso;
**Respuesta: Por el momento no.**

23. Informas sí se cuenta con documento de seguridad en materia de protección de datos personales:

**Respuesta: Actualmente, se encuentra en desarrollo, cabe señalar que de conformidad con el artículo 18 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Baja California, *"El responsable debe elaborar un documento de seguridad y actualizarlo conforme a los supuestos que enmarca la Ley General"*, mientras que el artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados establece los documentos que integran el Documento de Seguridad, consistentes en:**

***VIII. El inventario de datos personales y de los sistemas de tratamiento;***
***IX. Las funciones y obligaciones de las personas que traten datos personales;***
***X. El análisis de riesgos;***
***XI. El análisis de brecha;***
***XII. El plan de trabajo;***
***XIII. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y***
***XIV. El programa general de capacitación.***

**Con base en lo anterior, se informa que este Tribunal cuenta con:**

| Documento | Estado |
|---|---|
| 2. *El inventario de datos personales y de los sistemas de tratamiento;* | Proyecto en revisión |
| 9. *Las funciones y obligaciones de las personas que traten datos personales;* | Proyecto en revisión |
| 10. *El análisis de riesgos;* | Pendiente |
| 11. *El análisis de brecha;* | Pendiente |
| 12. *El plan de trabajo;* | Pendiente |
| 13. *Los mecanismos de monitoreo y revisión de las medidas de seguridad, y* | Pendiente, debido a que resultarán de las conclusiones del análisis de riesgos. |
| 14. *El programa general de capacitación.* | Proyecto 2025 en revisión |

32. Informar sí de conformidad con la Ley General de Protección de Datos Personales en Posesión de Particulares se cuenta con lo siguiente, un sistema de gestión de protección de datos personales, en caso de ser afirmativa esta pregunta, ¿desde cuándo se adoptó y cuáles áreas participaron en su desarrollo e implementación?:

**Respuesta: Respecto a este punto, se informa que la Ley Federal de Protección de Datos Personales en Posesión de Particulares, no es aplicable a Sujetos Obligados, de conformidad con los artículos 1 y 2 del mencionado ordenamiento; por lo tanto, no es aplicable a este Tribunal. A continuación, se transcriben los artículos para mayor comprensión:**

***"Artículo 1.- La presente Ley es de orden público y de observancia general en toda la República y tiene por objeto la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.***

***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."***

34. Informar sí se cuenta con un modelo o sistema de comunicación, para informar a la sociedad en general sobre los eventos o incidentes de seguridad de la institución, y en caso de ser afirmativo, ¿cuáles áreas de la institución que participan? e informar desde cuándo se implementó.
**Respuesta: Por el momento no se cuenta con un modelo o sistema de comunicación.**

35. Informar sobre sí se cuenta con un modelo o sistema de comunicación para informar a los titulares de datos personales en caso de brechas de seguridad de esta información, y señalar cuáles áreas de la organización participan en su implementación y desde cuándo se implementó:
**Respuesta: Por el momento no se cuenta con un modelo o sistema de comunicación.**

42. Informar sí se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son:
**Respuesta: Si; recientemente se ha incluido dentro del Portal Web del Tribunal, la siguiente página: https://tejabc.mx/solicitudesarco , en la cual de manera sencilla y amigable se pone a disposición de la ciudadanía los formatos que les permitirán ejercer sus derechos ARCO, presentar denuncias y recursos de revisión en esta materia. Asimismo, existe el apartado https://tejabc.mx/derechos-arco , mediante el cual se informa todo lo relacionado con el ejercicio de derechos ARCO, conceptos, requisitos, formatos, plazos, notificaciones, requisitos específicos, etc. Con estas dos herramientas digitales se facilita el ejercicio de derechos ARCO por parte de los titulares.**
**Por otra parte, en fecha 7 de noviembre de 2024, el Pleno de este Tribunal aprobó el Nuevo Catálogo de Protección de Datos Personales, criterios y resoluciones para su tratamiento (versión 2024), con lo cual se eleva el nivel de protección de los datos**

**personales pues los servidores públicos de este Tribunal pueden acudir a dicho documento para resolver dudas sobre toda aquella información que pudiera revestir la calidad de confidencial.**

43. Informar sí algún sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que se emplee implica el tratamiento intensivo y/o relevante de datos personales, de conformidad de la Ley en la materia; en caso afirmativo señalar sí se han llevado a cabo evaluaciones de impacto en materia de protección de datos personales; señalar cuáles han sido las recomendaciones vertidas por el del INAI, en su caso;
**Respuesta: Por el momento no.**

**En caso de inconformidad:**
Cuenta con un plazo de 15 días hábiles, contados a partir del día siguiente de la fecha de notificación de la presente respuesta, para presentar recurso de revisión ante el Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Baja California, a través de la Plataforma Nacional de Transparencia, http://www.plataformadetransparencia.org.mx/, en la sección denominada "Quejas de Respuestas", o bien, en forma escrita o mediante escrito libre, en el domicilio del Instituto.

**Dudas o aclaraciones:**
Si tiene alguna duda sobre el derecho de acceso a la información y/o de protección de datos personales o del proceso para presentar su inconformidad en contra de la presente respuesta, le sugerimos escribirnos al correo electrónico **transparencia@tejabc.mx** donde con mucho gusto le atenderemos.

Sin otro particular, aprovecho la ocasión para enviarle un cordial saludo.

**ATENTAMENTE**

**LIC. ZAYDA LORENA RODRIGUEZ BALCAZAR.**
**COORDINADORA DE TRANSPARENCIA**
**(TITULAR DE LA UNIDAD DE TRANSPARENCIA)**
**DEL TRIBUNAL ESTATAL DE JUSTICIA ADMINISTRATIVA**
**DE BAJA CALIFORNIA.**

TRIBUNAL ESTATAL DE JUSTICIA ADMINISTRATIVA DE BAJA CALIFORNIA
15 NOV 2024
DESPACHADO
COORDINACION DE TRANSPARENCIA
MEXICALI, B.C.

TRIBUNAL ESTATAL DE JUSTICIA ADMINISTRATIVA ESTADOS UNIDOS MEXICANOS BAJA CALIFORNIA
COORDINACIÓN DE TRANSPARENCIA
MEXICALI, B.C.

TE JA **TRIBUNAL ESTATAL DE JUSTICIA ADMINISTRATIVA**
BAJA CALIFORNIA

Mexicali, Baja California a 12 de noviembre de 2024.

**ASUNTO:** Solicitud de información **020068124000083.**

**Oficio: 52/2024.**

TE JA TRIBUNAL ESTATAL DE JUSTICIA ADMINISTRATIVA DE BAJA CALIFORNIA

12 NOV 2024
RECIBIDO
COORDINACIÓN DE TRANSPARENCIA
MEXICALI, B.C.

**ZAYDA LORENA RODRÍGUEZ BALCAZAR**
**COORDINADORA DE TRASPARENCIA DEL TRIBUNAL ESTATAL DE JUSTICIA ADMINISTRATIVA DE BAJA CALIFORNIA**
**P R E S E N T E.-**

Por este conducto, en respuesta a su oficio **TEJABC/CT/244/2024**, presentado ante la Coordinación de Sistemas Informáticos el veintidós de octubre del año en curso, mediante el cual se remitió la solicitud de información pública con número de folio **020068124000083**, en el cual se indica lo siguiente:"

***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;*
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 sí se cuenta con un 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.*
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;*
4. *Informar Sí se emplea la firma electrónica avanzada en la institución;*
5. *Informar sí se realizan simulacros sobre el plan de recuperación de desastres o en caso de incidentes cibernéticos;*

6. *Señalar sí se cuentan con lineamientos de programación y desarrollo de sistemas informáticos seguros;*
7. *Informar sí los servicios de centros de datos son propios, de otra institución gubernamental o de un tercero;*
8. *Informar sí para el trabajo remoto se cuentan con lineamientos de seguridad para las videollamadas;*
9. *Informar sí 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 sí se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información Institucional por parte de los servidores públicos;*
11. *Informar sí la página web de la institución cuenta con: a) aviso de privacidad; b) certificados digitales vigentes;*
12. *Informar sí el personal responsable se ha capacitado en la implementación del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos;*
13. *Informar sí 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 sí 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 sí 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 ésta pregunta, ¿desde cuándo se adoptó y cuáles áreas participaron en su desarrollo e implementación?;*
16. *Informar sí se cuenta con un modelo o sistema de comunicación, para informar a la sociedad en general sobre los eventos o incidentes de seguridad de la institución, y en caso de ser afirmativo, ¿cuáles áreas de la institución que participan? E informar desde cuándo se implementó;*
17. *Informar sobre sí se cuenta con un modelo o sistema de comunicación para informar a los titulares de datos personales en caso de brechas de seguridad de esta información, y señalar cuáles áreas de la organización participan en su implementación y desde cuándo se implementó;*
18. *Informar sí se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos;*
19. *Informar sí las personas encargadas de sistemas de información, donde se brinde información pública, cuentan con conocimientos comprobables en las siguientes*

*materias (i) transparencia; (ii) protección de datos personales; (iii) archivos públicos; o, (iv) seguridad de la información.*

20. *Informar sí han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas;*
21. *Informar sí se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son;*
22. *Informar sí algún sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que se emplee implica el tratamiento intensivo y/o relevante de datos personales, de conformidad de la Ley en la materia; en caso afirmativo señalar sí se han llevado a cabo evaluaciones de impacto en materia de protección de datos personales; señalar cuáles han sido las recomendaciones vertidas por el del INAI, en su caso;*
23. *Informar sí se cuenta con documento de seguridad en materia de protección de datos personales;*
24. *Informar sí 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 sí 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 sí las páginas web de los buscadores de versiones públicas de sentencias del Tribunal, tienen certificados digitales vigentes.*

***Solicito la siguiente información.***

29. *Informar sí dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan;*
30. *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;*
31.- *Informar sí se cuenta con un sistema de gestión de seguridad de la información dentro de la institución;*
32. *Informar sí de conformidad con la Ley General de Protección de Datos Personales en Posesión de Particulares se cuenta con lo siguiente, Un sistema de gestión de protección de datos personales, en caso de ser afirmativa esta pregunta, ¿desde cuándo se adoptó y cuáles áreas participaron en su desarrollo e implementación?;*
33. *Informar sí es que se cuenta con un plan de continuidad del negocio, para el caso de algún evento o incidente de seguridad cibernética o física e informar desde cuándo se implementó;*

34. *Informar sí se cuenta con un modelo o sistema de comunicación, para informar a la sociedad en general sobre los eventos o incidentes de seguridad de la institución, y en caso de ser afirmativo, ¿cuáles áreas de la institución que participan? E informar desde cuándo se implementó;*
35. *Informar sobre sí se cuenta con un modelo o sistema de comunicación para informar a los titulares de datos personales en caso de brechas de seguridad de esta información, y señalar cuáles áreas de la organización participan en su implementación y desde cuándo se implementó;*
36. *Informar sí se realiza capacitación continua a los servidores públicos en materia de ciberseguridad y cada cuando se lleva a cabo, así como los temas que se abordan;*
37. *Informar sí se cuenta con un procedimiento en caso de detección de alguna amenaza o vulneración de seguridad y cuál es el área en cargada de atender los reportes;*
38. *Informar sí se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos;*
39. *Informar sí las personas encargadas de sistemas de información, donde se brinde información pública, cuentan con conocimientos comprobables en las siguientes materias (i) transparencia (ii) protección de datos personales; (iii) archivos públicos; o, (iv) seguridad de la información.*
40. *Informar sí han tenido brechas de ciberseguridad desde el año 2014 a la fecha de la presente solicitud y señalar cuáles;*
41. *Informar sí se cuenta con un modelo de madurez de seguridad de la información o ciberseguridad dentro de la institución, en caso afirmativo informar desde cuándo se implementa;*
42. *Informar sí se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son;*
43. *Informar sí algún sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que se emplee implica el tratamiento intensivo y/o relevante de datos personales, de conformidad de la ley en la materia; en caso afirmativo señalar sí se han llevado a cabo evaluaciones de impacto en materia de protección de datos personales; señalar cuáles han sido las recomendaciones vertidas por el del INAI, en su caso;*
44. *Informar cada cuanto tiempo se actualizan las medidas de ciberseguridad dentro de la institución;*
45. *Informar sí se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como 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 aplicaban 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.*
    *d. 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 se selección y asignación aleatoria de casos?*
55. *¿Qué datos se utilizan para la sección y asignación aleatoria de casos?."(SIC)".*

**Respuesta:** En relación a la información solicitada se da repuesta a las preguntas.

**APARTADO 1**

1.-No

2.-

a).- En los archivos de esta Coordinación no se encontró algún archivo
c).- Si,
d).- Si-2018
e).- Si
f).- Si
g).- Si, Ingeniero externo 2015
h).- Si
i).-Si

3.-
i.- 2015
ii.- Se actualiza según las necesidades, de acuerdo a las nuevas tecnologías, de acuerdo a las nuevas amenazas de ciberseguridad
iii.- De acuerdo a la respuesta anterior
iv.- El Ingeniero externo

4.-Si

5.-Si, el Ingeniero externo

6.- En los archivos de esta Coordinación no se encontró algún archivo

7.- Si, propios

8.-En los archivos de esta Coordinación no se encontró algún archivo

9.-
a.- No
c.- Si
d.- Si
e.- Si

10.- En los archivos de esta Coordinación no se encontró algún archivo

11.- En los archivos de esta Coordinación no se encontró algún archivo

12.-En los archivos de esta Coordinación no se encontró algún archivo, pero el personal de la Coordinación de Sistemas Informáticos a leído el protocolo.

13.- a).- Si, ingeniero externo
b).-.No

14.- En los archivos de esta Coordinación no se encontró algún archivo

16.- En los archivos de esta Coordinación no se encontró algún archivo

17.- En los archivos de esta Coordinación no se encontró algún archivo

18.- En los archivos de esta Coordinación no se encontró algún archivo

19.- En los archivos de esta Coordinación no se encontró algún archivo
i).-
ii).-
iii).-

20.- No

21.- En los archivos de esta Coordinación no se encontró algún archivo

24.- No

25.- Se actualizan de acuerdo a las nuevas tecnologías es decir a las nuevas amenazas de ciberseguridad, con el ingeniero externo

26.- No

27.- Si, interno ingeniero externo

28.- Si ingeniero externo

29.- No

30.- Si

i.- 2015

ii.- Se actualiza según las necesidades, de acuerdo a las nuevas tecnologías, de acuerdo a las nuevas amenazas de ciberseguridad

iii.- De acuerdo a la respuesta anterior

iv.- El Ingeniero externo

31.- Si, Ingeniero externo

33.- Si, con el Ingeniero externo

34.- No En los archivos de esta Coordinación no se encontró algún archivo

35.- No En los archivos de esta Coordinación no se encontró algún archivo

36.- En los archivos de esta Coordinación no se encontró algún archivo

37.- Si, Firell

38.-En los archivos de esta Coordinación no se encontró algún archivo.

39.- En los archivos de esta Coordinación no se encontró algún archivo

40.- No

41.- No

42.- En los archivos de esta Coordinación no se encontró algún archivo

44.- Se actualizan de acuerdo a las nuevas tecnologías, es decir a las nuevas amenazas de ciberseguridad.

45.- No

46.- Si, Ingeniero externo

47.- Si, interno ingeniero externo

48.- Si, externo

**APARTADO 3**

49.- No

50.- No

51.- No, no creemos por el momento necesario la aplicación de inteligencia artificial para proporcionar el servicio al público.

52.- No

53.- No
a)
b)
c)

54.- No se puede proporcionar porque vulnera la seguridad

55.- Es un número con balance de cargas

**A T E N T A M E N T E**

**LIC. DIANA ADELA PÉREZ AMADOR**
**COORDINADORA DE SISTEMAS INFORMÁTICOS DEL TRIBUNAL ESTATAL DE JUSTICIA ADMINISTRATIVA DE BAJA CALIFORNIA**