

DIRECCIÓN DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA

La Paz, Baja California Sur, a 30 de octubre de 2024

Asunto: Se emite respuesta a la solicitud de información pública de folio 031158024000028

A QUIEN CORRESPONDA

Presente

Por medio del presente y dando seguimiento a la solicitud de acceso a la información pública de folio 031158024000028 realizada por usted a este Tribunal en fecha 21 de octubre de 2024, a través de la Plataforma Nacional de Transparencia, donde solicita lo siguiente:

“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;
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 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 INAI, en su caso;

44. Informar cada cuánto 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 su periodicidad;

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

47. Señalar si se cuenta con un help desk que recoja las incidencias reportadas por los servidores públicos, y en su caso señalar si es interno o externo.

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

APARTADO 3

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

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

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

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

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

a. Las fechas de operación.

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

c. Los contratos de su uso o adquisición.

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

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

Del estudio realizado a la solicitud de información presentada por usted, se advierte que la información peticionada corresponde a la **Unidad de Control Interno y Vigilancia Presupuestal de este Tribunal** y con base en la respuesta recibida en la Dirección de Transparencia a mi cargo, mediante el **oficio TEEBCS-UCIVP-40/2024** emitido por dicha unidad, se hace del conocimiento al solicitante lo siguiente:

En relación a lo solicitado, punto a punto, le comento lo siguiente:

Sobre el Apartado 1.

1. La unidad de control interno y vigilancia presupuestal no tiene conocimiento en organigrama sobre la existencia de un gobierno de seguridad de la información o ciberseguridad; en cuanto a la participación de áreas en los trabajos de seguridad de la información, todas las áreas de la institución colaboran en la protección a través de las disposiciones institucionales.

Anexo para ello el organigrama del TEEBCS:

<https://teebcs.mx/art-75-fraccion-ii/>

2. a) La institución se apeg a los procedimientos de ley para la adquisición de bienes, arrendamiento de bienes, o contratación de servicios, bajo los marcos aplicables.

b) La institución cuenta con inventario institucional de bienes y servicios; por tanto, los recursos tecnológicos existentes se encuentran incluidos, si se cuenta con alguno.

c) Se cuenta con los marcos jurídicos, manual de operaciones y todo lo relativo a la operatividad institucional, en particular, cada año se elabora el Plan Anual de Trabajo institucional.

d) De acuerdo con el número de lineamientos y reglamentaciones que tiene el Tribunal Estatal Electoral de Baja California Sur no se cuenta aún con un plan de recuperación de información ante desastres.

e) De acuerdo con el número de lineamientos y reglamentaciones que tiene el Tribunal Estatal Electoral de Baja California Sur no se cuenta aún con un plan de recuperación de información ante desastres.

f) No se cuenta en específico con el material en cuestión.

g) Se cuenta con políticas de seguridad de la información, apegadas al marco normativo aplicable, mismos que deben seguir todos los funcionarios públicos adscritos al TEEBCS, desde su primer día en su encargo.

h) Se tiene un manual de procedimientos, derivado de un diagnóstico de los procesos.

TRIBUNAL ESTATAL ELECTORAL

BAJA CALIFORNIA SUR

Puede visualizarse en:

<https://drive.google.com/file/d/1siVa1skAUq-5XCWjdVWmSmBkbvqk5zJ4/view>

- i) No se cuenta con un equipo especializado en esa materia.
- 3. Lo relativo a la ciberseguridad de la página y correos institucionales se encuentra a cargo del proveedor que presta dicho servicio.
- 4. La firma electrónica avanzada se utiliza en procesos judiciales particulares, en apego a las disposiciones legales conducentes.
- 5. Se tiene establecido el protocolo para informar al proveedor externo de ciberseguridad sobre incidentes, por tanto no se realizan simulacros.
- 6. No se cuentan con lineamientos de programación y desarrollo de sistemas informáticos seguros.
- 7. Los servicios de centros de datos no son propios.
- 8. Los servicios de videollamadas o difusión de información audiovisual es proporcionada por terceros; no obstante, se cuentan con lineamientos para el desarrollo de las sesiones públicas realizadas por videollamada:

Visible en:

https://drive.google.com/file/d/11giTlaYhnx6aZ8CVot0u8HtVW_XTsQC/view

- 9. Se cuenta con correo institucional, con dominio @teebcs.mx;
 - a) El uso de cualquier leyenda es de acuerdo a las disposiciones legales aplicables.
 - b) [No hay pregunta en la solicitud].
 - c) El servicio es prestado a través de un tercero.
 - d) El servicio brinda esos servicios.
 - e) El servicio brindado incluye ese servicio.
- 10. Si se cuenta con mecanismos, mismos que se encuentran alineados a las disposiciones legales vigentes en la materia.

11. La página web institucional cuenta con:
- a) Aviso de privacidad
 - b) Certificados digitales vigentes
12. No se ha llevado a cabo la capacitación señalada, de acuerdo con los datos que tiene esta Unidad de Control Interno y Vigilancia Presupuestal.
13. Respecto:
- a) Se cuentan con mecanismos de protección de la información.
 - b) Se cuentan con indicadores sobre los mecanismos de protección de la información.
14. No se cuenta con un Programa, pero se tienen disposiciones legales respecto al manejo de la información de conocimiento de los servidores públicos adscritos a la institución.
15. No se cuenta con un sistema informático para la gestión de protección de datos personales, pero se observan las leyes aplicables para el manejo interno de los datos personales.
16. Se cuenta con un sistema de información institucional, pero no uno especializado en temas de seguridad.
17. Se tienen institucionalizados todos los protocolos en materia de protección de datos, incluyendo situaciones particulares, de acuerdo a lo establecido en la normatividad vigentes, y los procedimientos se ajustan y establecen de acuerdo a lo señalado en la materia, desde el momento en que las disposiciones legales, acuerdos, normas, reglamentos y similares son publicadas y la institución se vuelve sujeta a su implementación.
18. Los lineamientos respecto a procedimientos administrativos y manejo de activos se tienen en el marco normativo contenido en la página institucional, <https://teebcs.mx/marco-normativo/>
19. Las personas encargadas de suministrar y manejar información, incluyendo información sensible, se apegan estrictamente a las disposiciones aplicables

TRIBUNAL ESTATAL ELECTORAL

BAJA CALIFORNIA SUR

en la materia y cuentan con capacitaciones, cursos y experiencia para el desarrollo de su actividad.

20.No se han tenido brechas de afectación a la ciberseguridad que tenga conocimiento esta unidad de control interno y vigilancia presupuestal.

21.Se lleva seguimiento de las reformas y disposiciones jurídicas aplicables en la materia de protección de datos personales.

22.No se cuenta con una plataforma propia que cumpla dichas características.

23.De acuerdo con la información de esta Unidad de Control Interno y Vigilancia Presupuestal, dicho documento se encuentra en elaboración.

24.No se cuenta con uno.

25.El servicio es contratado con un tercero.

26.El servicio es contratado con un tercero.

27.El servicio es contratado con un tercero.

28.El sitio web institucional cuenta con certificados digitales vigentes, además las versiones públicas de las sentencias se elaboran previo a ser cargadas directamente en la página institucional.

SOBRE EL APARTADO 2.

29.La unidad de control interno y vigilancia presupuestal no tiene conocimiento en organigrama sobre la existencia de un gobierno de seguridad de la información o ciberseguridad; en cuanto a la participación de áreas en los trabajos de seguridad de la información, todas las áreas de la institución colaboran en la protección a través de las disposiciones institucionales.

Anexo para ello el organigrama del TEEBCS:

<https://teebcs.mx/art-75-fraccion-ii/>

30.Lo relativo a la ciberseguridad de la página y correos institucionales se encuentra a cargo del proveer que presta dicho servicio.

31.Si se cuenta un servicio otorgado por tercero.

32.La institución cumple con las normas sobre protección de datos personales de acuerdo a las leyes aplicables, desde el mismo momento que entran en vigor, con los recursos que se encuentran disponibles.

33.No se cuenta con un plan institucional.

34.Se cuenta con un sistema de información institucional, pero no uno especializado en temas de seguridad.

35.Se tienen institucionalizados todos los protocolos en materia de protección de datos, incluyendo situaciones particulares, de acuerdo a lo establecido en la normatividad vigentes, y los procedimientos se ajustan y establecen de acuerdo a los señalado en la materia, desde el momento en que las disposiciones legales, acuerdos, normas, reglamentos y similares son publicadas y la institución se vuelve sujeta a su implementación.

36.Los temas de ciberseguridad son proveídos por un tercero.

10

37.Se cuenta con protocolos institucionales en temas de amenazas o vulneraciones a la seguridad de la institución; dichas situaciones son reportadas a la Secretaría General de Acuerdos.

38.Los lineamientos respecto a procedimientos administrativos y manejo de activos se tienen en el marco normativo contenido en la página institucional, <https://teebcs.mx/marco-normativo/>

39.Las personas encargadas de suministrar y manejar información, incluyendo información sensible, se apegan estrictamente a las disposiciones aplicables en la materia.

40.No se han tenido brechas de afectación a la ciberseguridad que tenga conocimiento esta unidad de control interno y vigilancia presupuestal.

41.No se cuenta con un modelo propio de ciberseguridad.

42.Se han aplicado todas las disposiciones legales y exigibles jurídicamente en lo relacionado con la protección de datos personales; en particular lo reséñate a las leyes sobre protección de datos vigentes en México.

TRIBUNAL ESTATAL ELECTORAL

BAJA CALIFORNIA SUR

43.No se cuenta con una plataforma propia que cumpla dichas características.

44.El servicio de ciberseguridad existente es suministrado por un proveedor de servicios externo.

45.El servicio de ciberseguridad existente es suministrado por un proveedor de servicios externo.

46.El servicio de ciberseguridad existente es suministrado por un proveedor de servicios externo.

47.El servicio de ciberseguridad existente es suministrado por un proveedor de servicios externo.

48.El servicio de ciberseguridad existente es suministrado por un proveedor de servicios externo.

SOBRE EL APARTADO 3.

11

49.No se cuenta con un sistema actualmente.

50.No se cuenta con un sistema actualmente.

51.No se tiene el conocimiento.

52.No se cuenta con un sistema actualmente.

53.No se cuenta con un sistema actualmente.

54.La única materia propia de este tribunal es la electoral. La asignación se realiza en orden alfabético y lo regula el artículo 232 del Reglamento Interno del Tribunal Estatal Electoral de Baja California Sur.

Visible en:

<https://drive.google.com/file/d/1wZ6hiPC2pdNvzNT5YzwDCiCmRNFLmYtU/view>

55.La aletoriedad de los casos se da por orden alfabético y lo regula el artículo 232 del Reglamento Interno del Tribunal Estatal Electoral de Baja California Sur.

TRIBUNAL ESTATAL ELECTORAL

BAJA CALIFORNIA SUR

Visible en:

<https://drive.google.com/file/d/1wZ6hiPC2pdNvzNT5YzwDCiCmRNFLmYtU/view>

Sin más por el momento, quedo a sus órdenes para cualquier duda o aclaración al respecto.

Atentamente


Lic. Domenica María Jiménez Osuna

**Directora de Transparencia y Acceso a la Información Pública
del Tribunal Estatal Electoral de Baja California Sur**