

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;
NO SE CUENTA CON NINGUNO, SOLO SE INSTALA ANTIVIRUS.
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.
NO SE CUENTA CON NINGUNO, NUESTRO PRESUPUESTO NO HA PERMITIDO DESARROLLAR, ADEMÁS QUE LA ENTIDAD NO HA REQUERIDO ALGUNO DE ELLOS PARA SU FUNCIONAMIENTO.
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 ;
NO APLICA
4. Informar sí se emplea la firma electrónica avanzada en la institución;
NO SE CUENTA, YA QUE NO SE HA BRINDADO EL PRESUPUESTO PARA LA COMPRA DEL SISTEMA.
5. Informar sí se realizan simulacros sobre el plan de recuperación de desastres o en caso de incidentes cibernéticos;
NO
6. Señalar si se cuentan con lineamientos de programación y desarrollo de sistemas informáticos seguros;
NO
7. Informar sí los servicios de centros de datos son propios, de otra institución gubernamental o de un tercero;
SON PROPIOS
8. Informar sí para el trabajo remoto se cuentan con lineamientos de seguridad para las videollamadas;
POR EL MOMENTO NOCONTAMOS CON LA MODALIDAD DE TRABAJO REMOTO

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.
SÍ SE CUENTA CON CORREO INSTITUCIONAL, PERO LOS DEMÁS INCISOS NO LOS IMPLEMENTAMOS.
10. Informar sí se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información Institucional por parte de los servidores públicos;
NO
11. Informar sí la página web de la institución cuenta con: a) aviso de privacidad; b) certificados digitales vigentes;
SÍ
12. Informar sí el personal responsable se ha capacitado en la implementación del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos;
NO SE HA BRINDADO YA QUE NO SE HA REQUERIDO
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;
NO SE CUENTA
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.
NO SE HA IMPLEMENTADO
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?;
POR EL MOMENTO NO SE HA IMPLEMENTADO
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;
Por el momento no, es de forma vía telefónica o en caso que se encuentren en las instalaciones con los teléfonos fijos. El área encargada es la Unidad Administrativa
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;
Por el momento no se cuenta con algún modelo o sistema.
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 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.
Por el momento no se nos ha brindado el presupuesto para la contratación de personal especializado. El personal mismo de otras áreas apoya con lo necesario para el cumplimiento de las obligaciones y se toman capacitaciones.
20. Informar si han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas;
No
21. Informar si se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son;
No
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;
Ninguno
23. Informas 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;
No
25. Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución;
Cada año
26. Informar si se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad;
No, por el momento no tenemos una autoridad responsable para revisar ese tema.
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.
No se cuenta con uno.
28. Señalar si las páginas web de los buscadores de versiones públicas de sentencias del Tribunal, tienen certificados digitales vigentes.
[https://tje-bc.gob.mx/sentencias/1730409715DIGITALJC237-2024SENTENCIA\[1\].pdf](https://tje-bc.gob.mx/sentencias/1730409715DIGITALJC237-2024SENTENCIA[1].pdf)
si se encuentran certificadas, anexo ejemplo descargado del portal
<https://tje-bc.gob.mx/sentencias.php>

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;
No se cuenta con un gobierno de seguridad.
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 ;
No se cuenta con alguna estrategia.
31. Informar sí se cuenta con un sistema de gestión de seguridad de la información dentro de la institución;
Solo antivirus.
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?;
Por el momento no se cuenta con un sistema de gestión.
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;
Por el momento no lo ha necesitado la institución, razón por el cual no se ha implementado.
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;
Por el momento no lo ha necesitado la institución, razón por el cual no se ha implementado.
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
Por el momento no lo ha necesitado la institución, razón por el cual no se ha implementado.
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;
No, por el momento la institución no cuenta con un presupuesto suficiente para implementar el tea de ciberseguridad, además por ser una entidad pequeña no se ha necesitado implementar ya que no se ha presentado problema alguno.

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;
Nos comunicamos con el Proveedores externo en caso de resultar alguna sospecha y se encarga de revisar
38. Informar si se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos;
Ninguno
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.
No, por el momento se toman capacitaciones solamente.
40. Informar si han tenido brechas de ciberseguridad desde el año 2014 a la fecha de la presente solicitud y señalar cuántas;
Ninguna
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;
Por el momento no se cuenta por falta de recurso y no se ha necesitado por la entidad.
42. Informar si se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son;
Por el momento no se cuenta por falta de recurso y no se ha necesitado por la entidad.
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;
Cada año nos realiza una evaluación por el momento no nos ha solicitado alguna mejora o recomendación.
44. Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución;
Cada año
45. Informar si se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad;
Ninguna
46. Señalar si se cuenta con un sistema de gestión de incidentes y cuáles áreas de la institución participan en este;
No se cuenta con un sistema
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.
Ninguno
48. Señalar si se cuenta con un equipo de respuesta a incidentes cibernéticos, especificar si es interno o externo. Ninguno

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. Por el momento se necesita presupuesto para implementar, como primer paso pero no se ha otorgado.

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. Por el momento contar con el presupuesto suficiente.

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.

En el tribunal electoral está conformado por magistrados, y se turnan los expediente por orden alfabético.

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.*

No utilizamos ningún programa.

54. ¿Cómo procede y opera la selección y asignación aleatoria de casos a los jueces y juzgados en todas las materias?

Esto del corresponder al Tribunal del Poder Judicial del Estado de Baja California

¿Cómo se garantiza la independencia judicial a través de estos sistemas de selección y asignación aleatoria de casos?

Se lleva un registro de los turnos asignados y es mediante un oficio que se le notifica a cada magistrado.

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

Apellidos en orden alfabético.