

TRIBUNAL ELECTORAL TEEO DEL ESTADO DE OAXACA

Oficio número: TEEO/UT/158/2024.

Asunto: Se emite contestación.

Oaxaca de Juárez, Oaxaca, 05 de noviembre de 2024.

A QUIEN CORRESPONDA.

El que suscribe Licenciado Pascual Ríos Vázquez, Titular de la Unidad de Transparencia, del Tribunal Electoral del Estado de Oaxaca, con fundamento en lo dispuesto por los artículos 8 de la Constitución Política de los Estados Unidos Mexicanos; 3, párrafo décimo segundo, y 114 Bis, de la Constitución Política del Estado Libre y Soberano de Oaxaca, en relación con los artículos 1, 2, 6, fracciones I y XX, 7, fracción VI y 10, fracción IV, de la Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno del Estado de Oaxaca, manifiesto lo siguiente:

Por este medio, me permito darle contestación a su solicitud de acceso a la información pública, recibida vía Sistema de Solicitudes de Información, de la Plataforma Nacional de Transparencia, con número de folio 201173024000031, consistente en diversa información relacionada en su petición.

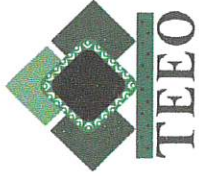
Al respecto, adjunto el oficio número TEEO/P/USI/67, suscrito por el Jefe de la Unidad de Sistemas Informáticos de este órgano jurisdiccional, conteniendo la respuesta correspondiente.

Así mismo, con respecto a la pregunta número "15. *Informar si de conformidad con la Ley General de Protección de Datos Personales en Posesión de Sujetos obligados se cuenta con un sistema de gestión de protección de datos personales, en caso de ser afirmativa esta pregunta, ¿desde cuándo se adoptó y cuáles áreas participaron en su desarrollo e implementación?...?*", se le hace de su conocimiento que no se cuenta.

Con respecto a la pregunta "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...*", se le informa que si se cuenta con conocimientos.

En relación a la pregunta "21. *Informar si se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son...*", se le informa que si se han adoptado en casos de violencia política en razón de género.

Con respecto a la pregunta "23. *Informar si se cuenta con documento de seguridad en materia de protección de datos personales...*", se le informa que no se cuenta.



TRIBUNAL ELECTORAL DEL ESTADO DE OAXACA

Con respecto a la pregunta "32. Informar si de conformidad con la Ley General de Protección de Datos Personales en Posesión de Particulares se cuenta con lo siguiente *Un sistema de gestión de protección de datos personales*, en caso de ser afirmativa esta pregunta, ¿desde cuándo se adoptó y cuáles áreas participaron en su desarrollo e implementación?... ", se le informa que no se cuenta.

Con respecto a la pregunta "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...", se le informa que si se cuenta con conocimientos.

Con respecto a la pregunta "42. Informar si se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son...", se le informa que si se han adoptado en casos de violencia política en razón de género.

Finalmente, con respecto a la pregunta "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...", se le informa que no se cuenta; lo anterior, para los efectos legales a que haya lugar.

Sin otro asunto en particular, y una vez solventada su solicitud, no me resta más que enviarle un cordial saludo.

ATENTAMENTE
SUFRAGIO EFECTIVO. NO REELECCIÓN
"EL RESPETO AL DERECHO AJENO ES LA PAZ"

Tribunal Electoral
del Estado de Oaxaca
Unidad de Transparencia



Oaxaca de Juárez, Oaxaca a 05 de noviembre del 2024
Of. N°. TEEO/P/USI/67

ASUNTO: Solicitud de Información Pública

Lic. Pascual Rios Vásquez
Titular de la Unidad de Transparencia del
Tribunal Electoral del Estado de Oaxaca.

En atención al oficio TEEO/UT/154/2024, donde solicita colaboración para recabar información solicitada a través de la plataforma Nacional de Transparencia, me permito anexar al presente la solicitud de información contestada, sin embargo, las preguntas marcadas en color rojo no son de mi competencia o en su caso desconozco.

Se anexan pues, las preguntas de la solicitud de información pública, así como también las preguntas del anexo nombrado: “PREGUNTAS TIC 2024”.

Sin más por el momento, quedo a sus órdenes y atento a sus comentarios.

A T E N T A M E N T E

MTRO. ESTEBAN BLADIMIR HERNÁNDEZ MARTÍNEZ
JEFE DE LA UNIDAD DE SISTEMAS INFORMÁTICOS
TRIBUNAL ELECTORAL DEL ESTADO DE OAXACA

C.e.p Maestra Elizabeth Bautista Velasco. – Magistrada Presidenta del Tribunal Electoral del Estado de Oaxaca. -Para su superior conocimiento.



**Tribunal Electoral
del Estado de Oaxaca
UNIDAD DE
SISTEMAS
INFORMÁTICOS**

PREGUNTAS

APARTADO 1

1. Informar si dentro de la institucion se cuenta con un gobierno de seguridad de la informacion o ciberseguridad y cuales areas participan;

R=NO SE CUENTA

2. Señalar si se cuenta con lo siguiente: a) un marco de mejores prácticas aplicables a la gestión de las TIC en los diferentes procesos de contratación para la adquisición, el arrendamiento de bienes o la prestación de servicios en materia de TIC y de seguridad de la información; Informar si se cuenta con una Inventario Institucional de bienes y servicios de TIC; c) un plan de continuidad de operaciones, y señalar la fecha de implementación; d) Informar si se ha desarrollado e implementado el plan de recuperación ante desastres, señalar la fecha de desarrollo e implementación; e) desarrollado e implementado un programa de gestión de vulnerabilidades; f) Marco de Gestión de Seguridad de la Información (MGSI) o Sistema de Gestión de Seguridad de la Información (SGSI); g) Informar si se cuenta con una política general de seguridad de la información y en su caso, quienes intervienen y desde cuándo se implementó; h) Informar si se cuenta con un diagnóstico de identificación de los procesos y activos esenciales de la Institución; i) Informar si se cuenta con un Equipo de Respuesta a Incidentes de Seguridad de la Información (ERISC) o Equipo de respuesta a Incidentes Cibernéticos o en su caso SOC.

R=NO SE CUENTA

3. Informar si es que se cuenta con una estrategia de ciberseguridad dentro de la institucion, en caso de respuesta afirmativa, informar lo siguiente (i) referir la fecha de creacion; (ii) la fecha de implementacion, (iii) si es que se ha actualizado o modificado y en cuantas ocasiones; (iv) cuales areas participaron en la creacion de dicha estrategia ;

R=NO SE CUENTA

4. Informar si se emplea la firma electronica avanzada en la institucion;

R=NO SE CUENTA

5. Informar si se realizan simulacros sobre el plan de recuperacion de desastres o en caso de incidentes ciberneticos;

R=NO SE REALIZAN

6. Señalar si se cuentan con lineamientos de programacion y desarrollo de sistemas informaticos seguros;

R=NO SE CUENTA

7. Informar si los servicios de centros de datos son propios, de otra institución gubernamental o de un tercero;
R=SON PROPIOS
8. Informar si para el trabajo remoto se cuentan con lineamientos de seguridad para las videollamadas;
R=NO SE CUENTA
9. Informar si se cuenta con un correo electrónico institucional; e Informar si el correo electrónico que se emplea en la institución cuenta con lo siguiente: a) Inserción de leyenda de confidencialidad de la información o en su caso de transparencia y acceso a la información; c) control institucional de la totalidad de los correos contenidos en las carpetas de los usuarios; d) Soluciones de filtrado para correo no deseado o correo no solicitado, así como programas informáticos que protejan del envío y recepción de correos electrónicos con software malicioso; e) cuenta con cifrado en el envío de información.
R=SI SE CUENTA CON CORREO ELECTRÓNICO
a) *R=NO SE CUENTA*
b)
c) *R=NO SE CUENTA*
d) *R=NO SE CUENTA*
10. Informar si se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información institucional por parte de los servidores públicos
R=NO SE CUENTA
11. Informar si la página web de la institución cuenta con: a) aviso de privacidad; b) certificados digitales vigentes;
a) *SI SE CUENTA*
b) *SI CUENTA*
12. Informar si el personal responsable se ha capacitado en la implementación del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos;
R=NO SE HA HECHO
13. Informar si se cuentan con: a) Los mecanismos de supervisión y evaluación que permitan medir la efectividad de los controles de seguridad de la información; b) Indicadores que permitan medir el madurez institucional en la gestión de seguridad de la información;
R=NO SE CUENTA

14. Informar si dentro de la institución se cuenta con un Programa de formación en la cultura de la seguridad de la información o de ciberseguridad; y en caso afirmativo señalar: cuándo se implementó.
R=NO SE CUENTA
15. Informar si de conformidad con la Ley General de Protección de Datos Personales en Posesión de Sujetos obligados se cuenta con un sistema de gestión de protección de datos personales, en caso de ser afirmativa esta pregunta, ¿desde cuándo se adoptó y cuáles áreas participaron en su desarrollo e implementación?;
16. Informar si se cuenta con un modelo o sistema de comunicación, para informar a la sociedad en general sobre los eventos o incidentes de seguridad de la institución, y en caso de ser afirmativo, ¿cuáles áreas de la institución que participan? e informar desde cuándo se implementó;
R=NO SE CUENTA
17. Informar sobre si se cuenta con un modelo o sistema de comunicación para informar a los titulares de datos personales en caso de brechas de seguridad de esta información, y señalar cuáles áreas de la organización participan en su implementación y desde cuándo se implementó;
R=NO SE CUENTA
18. Informar si se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos;
R=NO SE CUENTA
19. Informar si las personas encargadas de sistemas de información, donde se brinde información pública, cuentan con conocimientos comprobables en las siguientes materias (i) transparencia; (ii) protección de datos personales; (iii) archivos públicos; o, (iv) seguridad de la información.
20. Informar si han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas;
R=NO SE HAN TENIDO

21. Informar si se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son;
22. Informar si algún sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que se emplee implica el tratamiento intensivo y/o relevante de datos personales, de conformidad de la Ley en la materia; en caso afirmativo señalar si se han llevado a cabo evaluaciones de impacto en materia de protección de datos personales; señalar cuáles han sido las recomendaciones vertidas por el del INAI, en su caso;
R=NO SE CUENTA
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;
R=NO SE CUENTA
25. Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución;
R=CADA AÑO
26. Informar si se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad;
R=NO SE CUENTAN
27. Señalar si se cuenta con un help desk que recoja las incidencias reportadas por los servidores públicos, y en su caso señalar si es interno o externo.
R=NO SE CUENTA
28. Señalar si las páginas web de los buscadores de versiones públicas de sentencias del Tribunal, tienen certificados digitales vigentes.
R=SI CUENTAN

APARTADO 2

Solicito la siguiente información.

29. Informar si dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan;
R=NO SE CUENTA

30. Informar si es que se cuenta con una estrategia de ciberseguridad dentro de la institución, en caso de respuesta afirmativa, informar lo siguiente (i) referir la fecha de creación; (ii) la fecha de implementación, (iii) si es que se ha actualizado o modificado y en cuántas ocasiones; (iv) cuáles áreas participaron en la creación de dicha estrategia ;
R=NO SE CUENTA

31. Informar si se cuenta con un sistema de gestión de seguridad de la información dentro de la institución;
R=NO SE CUENTA

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

33. Informar si es que se cuenta con un plan de continuidad del negocio, para el caso de algún evento o incidente de seguridad cibernética o física e informar desde cuándo se implementó;
R=NO SE CUENTA

34. Informar si se cuenta con un modelo o sistema de comunicación, para informar a la sociedad en general sobre los eventos o incidentes de seguridad de la institución, y en caso de ser afirmativo, ¿cuáles áreas de la institución que participan? e informar desde cuándo se implementó;
R=NO SE CUENTA

35. Informar sobre si se cuenta con un modelo o sistema de comunicación para informar a los titulares de datos personales en caso de brechas de seguridad de esta información, y señalar cuáles áreas de la organización participan en su implementación y desde cuándo se implementó;
R=NO SE CUENTA

36. Informar si se realiza capacitación continua a los servidores públicos en materia de ciberseguridad y cada cuándo se lleva a cabo, así como los temas que se abordan;
R=NO SE CUENTA
37. Informar si se cuenta con un procedimiento en caso de detección de alguna amenaza o vulneración de seguridad y cuál es el área encargada de atender los reportes;
R=NO SE CUENTA
38. Informar si se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos;
R=NO SE CUENTA
39. Informar si las personas encargadas de sistemas de información, donde se brinde información pública, cuentan con conocimientos comprobables en las siguientes materias (i) transparencia; (ii) protección de datos personales; (iii) archivos públicos; o, (iv) seguridad de la información.
40. Informar si han tenido brechas de ciberseguridad desde el año 2014 a la fecha de la presente solicitud y señalar cuántas;
R=NO SE
41. Informar si se cuenta con un modelo de madurez de seguridad de la información o ciberseguridad dentro de la institución, en caso afirmativo informar desde cuándo se implementa;
R=NO SE CUENTA
42. Informar si se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son;
43. Informar si algún sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que se emplee implica el tratamiento intensivo y/o relevante de datos personales, de conformidad de la ley en la materia; en caso afirmativo señalar si se han llevado a cabo evaluaciones de impacto en materia de protección de datos personales; señalar cuáles han sido las recomendaciones vertidas por el del INAI, en su caso;
44. Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución;
R=CADA AÑO
45. Informar si se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad;
R=NO SE CUENTA

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

R=NO SE CUENTA

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

R=NO SE CUENTA

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

R=NO SE CUENTA

APARTADO 3

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

R=NO SE CUENTA

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

R=NO SE CUENTA

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

R=NO SE TIENE CONOCIMIENTO

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

R=NO SE CUENTA

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

- a. Las fechas de operación.
- b. El funcionamiento y operación de cada sistema o algoritmo con el que cuenta.
- c. Los contratos de su uso o adquisición.

R=NO SE CUENTA

54. *¿Cómo procede y opera la selección y asignación aleatoria de casos a los jueces y juzgados en todas las materias? ¿Cómo se garantiza la independencia judicial a través de estos sistemas de selección y asignación aleatoria de casos?*
R=NO SE CUENTA

55. *¿Qué datos se utilizan para la selección y asignación aleatoria de casos? (sic)*
R=NO SE CUENTA