

"2024, BICENTENARIO DE LA INTEGRACIÓN DE OAXACA A LA REPÚBLICA MEXICANA"

## TRIBUNAL ELECTORAL TEEO DEL ESTADO DE OAXACA

Oficio número: TEEO/UT/162/2024.

Asunto: Se emite contestación.

Oaxaca de Juárez, Oaxaca, 12 de noviembre de 2024.

Qt.

El que suscribe Licenciado Pascual Rios Vásquez, 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:

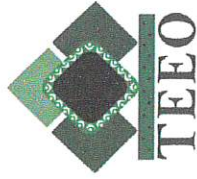
Por este medio, me permito darle contestación a su solicitud de acceso a la información pública, recibida vía Sistema de Solicitudes de Información, de la Plataforma Nacional de Transparencia, con número de folio 201173024000035, consistente en diversa información relacionada en su petición.

Al respecto, adjunto el oficio número TEEO/P/USI/68, 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 "14. 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 "18. 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 "20. 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.



"2024, BICENTENARIO DE LA INTEGRACIÓN DE OAXACA A LA REPÚBLICA MEXICANA"

## TRIBUNAL ELECTORAL DEL ESTADO DE OAXACA

Finalmente, con respecto a la pregunta "22. *Informar si se cuenta con documento de seguridad en materia de protección de datos personales...*", 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 11 de noviembre del 2024  
Of. N°. TEEO/P/USI/68

**ASUNTO:** Solicitud de Información Pública

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

En atención al oficio TEEO/UT/155/2024, 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.

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**



**Trámite Electoral**  
**UNIDAD 47 DE**  
**SISTEMAS**  
**INFORMÁTICOS**

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





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

**NO SE CUENTA**

2. Señalar si de conformidad con el Acuerdo por el que se emiten políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y la comunicación, y la seguridad de la información en la Administración Pública Federal, publicado en DOF el 6 de septiembre de 2021, se han implementado las siguientes medidas: a) estándares técnicos definidos por la Coordinación de Estrategia Digital Nacional, en la contratación de bienes y servicios seguridad de la información o de tecnologías de la información y comunicación;

**NO SE HA IMPLEMENTADO**

b) 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;

**NO SE CUENTA**

c) un plan de continuidad de operaciones, y señalar la fecha de implementación;

**NO SE CUENTA**

d) Informar si se ha desarrollado implementado el plan de recuperación ante desastres, señalar la fecha de desarrollo e implementación;

**NO SE CUENTA**

e) desarrollado e implementado un programa de gestión de vulnerabilidades;

**NO SE CUENTA**

f) Marco de Gestión de Seguridad de la Información (MGSI);

**NO SE CUENTA**





g) Informar sí se cuenta con una política general de seguridad información y en su caso, quienes intervienen y desde cuándo se implementó;

**NO SE CUENTA**

h) informar si se cuenta con un diagnóstico de identificación de los procesos y activos esenciales de la Institución;

**NO SE CUENTA**

i) Informar se cuenta con un Equipo de Respuesta a Incidentes de Seguridad de la Información (ERISC).

**NO SE CUENTA**

3. Informar sí es que se cuenta con una estrategia de ciberseguridad dentro de la institución, en cas respuesta afirmativa, informar lo siguiente (i) referir la fecha de creación; (ii) la fecha de implementac (iii) sí es que se ha actualizado o modificado y en cuántas ocasiones; (iv) cuáles áreas participaron e creación de dicha estrategia ;

4. Informar sí se emplea la firma electrónica avanzada en la institución;

**NO SE EMPLEA**

5. Informar sí se realizan simulacros sobre el plan de recuperación de desastres o en caso de incide cibernéticos;

**NO SE REALIZAN**





6. Señalar sí en la contratación de servicios de seguridad de la información en Tecnologías de la Información y Comunicación y Seguridad de la Información, de ha contado con el Dictamen Técnico favorable expedido por la CEDN, de conformidad con el Acuerdo por el que se emiten políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y la comunicación, y la seguridad de la información en la Administración Pública Federal, publicado en el DOF el 6 de septiembre de 2021

**NO SE CUENTA**

7. Informar si los servicios de centros de datos son propios, de otra institución gubernamental o de un tercero;  
**SON PROPIOS**

8. Informar si se cuenta con un correo electrónico institucional; e Informar si el correo electrónico que emplea en la institución cuenta con lo siguiente: a) inserción de leyenda de confidencialidad de 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 programa informáticos que protejan del envío y recepción de correos electrónicos con software malicioso; e) cuenta con cifrado en el envío de información.

**SI SE CUENTA CON CORREO ELECTRÓNICO INSTITUCIONAL**

- a) **NO SE CUENTA**
- b)
- c) **NO SE CUENTA**
- d) **NO SE CUENTA**

9. Informar si se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información Institucional por parte de los servidores públicos;

**NO SE CUENTA**

10. Informar si la página web de la institución cuenta con: a) aviso de privacidad; b) certificados digitales vigentes;

- a) **SI CUENTA**
- b) **SI CUENTA**





11. Informar si el personal responsable se ha capacitado en la implementación del protocolo nacional homologado para la gestión de incidentes cibernéticos.

**NO SE HA HECHO.**

12. 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;

**NO SE CUENTA**

b) Indicadores que permitan medir el madurez institucional en la gestión de seguridad de la información;

**NO SE CUENTA**

13. 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 y cuántas horas de capacitación en ciberseguridad se realizan de forma anual.

**NO SE CUENTA**

14. 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?;

15. 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, ¿cuales áreas de la institución que participan? e informar desde cuándo se implementó, lo anterior en términos de lo establecido por el artículos 40, 41 y 42 de la Ley general de protección de datos personales en posesión de sujetos obligados (LGPDPPSO):

**NO SE CUENTA**





16. 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, o anterior en términos de lo establecido por el artículos 40, 41 y 42 de la Ley general de protección de datos personales en posesión de sujetos obligados (LGPDPPSO));

**NO SE CUENTA**

17. Informar si se cuenta con lineamientos para el traslado de activos físicos(dispositivos móviles) de la institución, por parte de los servidores públicos;

**NO SE CUENTA**

18. 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.

19. Informar si han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas;

**NO SE HAN TENIDO**

20. Informar si se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son;





21. Informar si algún sistema o plataforma informática, aplicación electrónica o cualquier otro: 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;

**NO SE CUENTA**

22. Informar si se cuenta con documento de seguridad en materia de protección de datos personales;

23. Informar si se cuenta con un plan de comunicación institucional en caso de un incidente de ciberseguridad o seguridad de la información;

**NO SE CUENTA**

24. Informar cada cuánto tiempo de actualización las medidas de ciberseguridad dentro de la institución;

**CADA AÑO**

25. Informar si se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad;

**NO SE CUENTA**

26. Señalar si se cuenta con un help desk que recoja las incidencias reportadas por los servicios públicos, y en su caso señalar si es interno o externo. Un help desk es un equipo centralizado dentro de una empresa que atiende incidencias y reportes de sistemas informáticos y software de una organización.

**NO SE CUENTA**

27. Informar si se cuenta con un Centro de Operaciones de Ciberseguridad. Además informar si han tenido incidentes de ciberseguridad (sin importar ni decir cuáles)

**NO SE CUENTA**