

Tlaxcala de Xicohténcatl, a cinco de noviembre de dos mil veinticuatro.

VISTA la solicitud de información pública con número de folio **292165724000061**, constante de tres fojas útiles tamaño carta, escritas por su lado anverso, formulada a través del Sistema de Solicitudes de la Plataforma Nacional de Transparencia, a las quince horas con veintiséis minutos del treinta de octubre de dos mil veinticuatro, misma que fue recibida en esta Unidad de Transparencia y Protección de Datos Personales, a las nueve horas con cuarenta y tres minutos del cinco de noviembre de dos mil veinticuatro, **SE ACUERDA:**

RADICACIÓN. Con fundamento en el artículo 6 de la Constitución Política de los Estados Unidos Mexicanos, 97 bis, de la Constitución Política del Estado Libre y Soberano de Tlaxcala; 1, 4, 6, 8, 16, 17, 121, 124 y 136 de la Ley General de Transparencia y Acceso a la Información Pública; 1, 4, 6, 16, 17, 24, 41 fracciones II, IV y V, 53, 116, 117, 121, 122, 123 y 124 de la Ley de Transparencia y Acceso a la Información Pública del Estado; con la solicitud de información con número de folio **292165724000061**, **fórmese Expediente de Acceso a Información Pública bajo el número 48/2024**, de los del índice de la Unidad de Transparencia y Protección de Datos Personales del Tribunal de Justicia Administrativa del Estado de Tlaxcala, y **regístrese** en el Libro correspondiente que se lleva en esta Unidad, en virtud de que le corresponde recibir y dar trámite a la correspondiente solicitud de acceso a la información pública.

SOLICITUD DE INFORMACIÓN PÚBLICA. Este órgano jurisdiccional como sujeto obligado debe garantizar el derecho humano de acceso a la información de todas las personas en igualdad de condiciones, por tanto, analizada que fue la solicitud de información, mediante la cual se pide lo siguiente:

(...)

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

2. Señalar sí 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, se han implementado las siguientes medidas: a) estándares técnicos definidos por la Coordinación de Estrategia Digital Nacional, en la contratación de bienes y servicios de seguridad de la información o de tecnologías de la información y comunicación; 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 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); 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).

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 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

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

8. 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; 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.

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

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

11. Informar si el personal responsable se ha capacitado en la implementación del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos;

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

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

14. 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?;

15. 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, 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);

16. 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, 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);

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

18. 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.

19. Informar si han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas;
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 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;
22. Informas 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;
24. Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución;
25. Informar si se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad;
26. 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. Un help desk es un equipo centralizado dentro de una empresa que atiende incidencias y reportes de sistemas informáticos y software de una organización
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)
- (...)

CONSIDERACIONES PREVIAS. Este sujeto obligado estima pertinente señalar lo siguiente:

I. Que este órgano jurisdiccional como sujeto obligado se constituyó y entró en funciones el día diecisiete de septiembre del año dos mil dieciocho, según se desprende del Acta de Sesión Pública Solemne de Instalación del Tribunal de Justicia Administrativa y la designación de su Presidente, misma que puede consultarse en la liga electrónica: http://www.tjaet.gob.mx/docs/fracciones//acta_instalacion_tja_tlx.pdf;

Organismo Público Especializado en su momento parte del Poder Judicial del Estado, posteriormente mediante decreto número 247 publicado el treinta y uno de octubre de dos mil veintitrés en el Periódico Oficial del Estado, en su artículo 97 BIS, se estableció "El Tribunal de Justicia Administrativa del Estado de Tlaxcala, es un órgano jurisdiccional, dotado de plena autonomía, con personalidad jurídica y patrimonio propio, será independiente de cualquier autoridad"; de lo anterior resulta claro que a partir de su constitución, surgió la obligación de este de transparentar, permitir el acceso a su información y proteger los datos personales que obren en su poder, toda vez que no es posible generar información anterior a que iniciara funciones este Tribunal.

II. El Tribunal de Justicia Administrativa del Estado de Tlaxcala, se encuentra facultado para dirimir las controversias de carácter administrativo y fiscal que se susciten entre la administración pública estatal y municipal con los particulares y será el órgano competente para imponer, en los términos que disponga la ley, las sanciones a los servidores públicos estatales y municipales por responsabilidad administrativa grave, a los particulares que incurran en actos vinculados con faltas administrativas graves; así como para fincar a los responsables el pago de las indemnizaciones y sanciones pecuniarias que deriven de los daños y perjuicios que afecten a la hacienda pública Estatal o Municipal, o bien, al patrimonio de los entes públicos estatales o municipales, en los términos que establezca la legislación correspondiente, tal como lo establecen los artículos 97 Bis de la Constitución Política del Estado Libre y Soberano de Tlaxcala, 124 y 125

de la Ley del Procedimiento Administrativo del Estado de Tlaxcala y sus Municipios.

III. Los artículos 3, fracción VIII y 4, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tlaxcala, señalan:

1. Deberá entenderse por "Documento": Los expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas o bien, cualquier otro registro que documente el ejercicio de las facultades, funciones y competencias de los sujetos obligados, sus servidores públicos e integrantes, sin importar su fuente o fecha de elaboración;
2. El derecho humano de acceso a la información comprende solicitar, investigar, difundir, buscar y recibir información; y,
3. Toda la información generada, obtenida, adquirida, transformada o en posesión de los sujetos obligados es pública y accesible a cualquier persona en los términos y condiciones que se establezcan en la Ley Local, en la Ley General, en los tratados internacionales de los que el Estado mexicano sea parte, y la normatividad aplicable en sus respectivas competencias.

En ese orden, se advierte que las solicitudes de acceso a la información van encaminadas al suministro de un documento en concreto y preexistente, generado, obtenido, adquirido, transformado o en posesión del sujeto obligado.

CLASIFICACIÓN DE INFORMACIÓN. Los artículos 25 fracción VI¹, 40 fracción II², 92 párrafos primero y tercero³, 98 fracciones I, II y III⁴, 105 fracciones I, II, III, IV, V, VI, VII, VIII, IX y X⁵, 108 párrafo primero⁶, de la Ley de Transparencia y Acceso a la Información, señalan que:

- Es obligación de los sujetos obligados proteger y resguardar la información clasificada como reservada o confidencial;

¹ Artículo 25. Para el cumplimiento de los objetivos de esta Ley, los sujetos obligados deberán cumplir con las siguientes obligaciones, según corresponda, de acuerdo a su naturaleza:

VI. Proteger y resguardar la información clasificada como reservada o confidencial;

² Artículo 40. Los comités de transparencia tendrán las siguientes funciones:

II. Confirmar, modificar o revocar las determinaciones que en materia de ampliación del plazo de respuesta, clasificación de la información y declaración de inexistencia o de incompetencia realicen los titulares de las áreas de los sujetos obligados;

³ Artículo 92. La clasificación es el proceso mediante el cual el sujeto obligado determina que la información en su poder actualiza alguno de los supuestos de reserva o confidencialidad, de conformidad con lo dispuesto en el presente Título.

...

Los titulares de las áreas de los sujetos obligados serán los responsables de clasificar la información, de conformidad con lo dispuesto en esta Ley y la Ley General.

⁴ Artículo 98. La clasificación de la información se llevará a cabo en el momento en que:

I. Se reciba una solicitud de acceso a la información;
II. Se determine mediante resolución de autoridad competente, o
III. Se generen versiones públicas para dar cumplimiento a las obligaciones de transparencia previstas en esta Ley.

⁵ Artículo 105. Como información reservada podrá clasificarse aquella cuya publicación:

I. Comprometa la seguridad pública;
II. Pueda menoscabar la conducción de las negociaciones y relaciones internacionales;
III. Pueda poner en riesgo la vida, seguridad o salud de una persona física;
IV. Obstruya las actividades de verificación, inspección y auditoría relativas al cumplimiento de las leyes o afecte la recaudación de contribuciones;
V. Obstruya la prevención o persecución de los delitos;
VI. La que contenga las opiniones, recomendaciones o puntos de vista que formen parte del proceso deliberativo de los servidores públicos, hasta en tanto no sea adoptada la decisión definitiva, la cual deberá estar documentada;
VII. Obstruya los procedimientos para fincar responsabilidad a los servidores públicos, en tanto no se haya dictado la resolución administrativa;
VIII. Afecte los derechos del debido proceso;
IX. Vulnere la conducción de los expedientes judiciales o de los procedimientos administrativos seguidos en forma de juicio, en tanto no hayan causado estado;
X. Se encuentre contenida dentro de las investigaciones de hechos que la ley señale como delitos y se tramiten ante el Ministerio Público.

⁶ Artículo 108. Se considera información confidencial la que contiene datos personales concernientes a una persona identificada o identificable.

- Los comités de transparencia tendrán entre sus funciones confirmar, modificar o revocar las determinaciones que, en materia de ampliación del plazo de respuesta, clasificación de la información y declaración de inexistencia o de incompetencia realicen los titulares de las áreas de los sujetos obligados;
- La clasificación es el proceso mediante el cual el sujeto obligado determina que la información en su poder actualiza alguno de los supuestos de reserva o confidencialidad, y los titulares de las áreas de los sujetos obligados serán los responsables de clasificar la información;
- La clasificación de la información se llevará a cabo en el momento en que:
 - Se reciba una solicitud de acceso a la información.
 - Se determine mediante resolución de autoridad competente.
 - Se generen versiones públicas para dar cumplimiento a las obligaciones de transparencia previstas en esta Ley.
- Como **información reservada** podrá clasificarse aquella cuya publicación:
 - Comprometa la seguridad pública;
 - Pueda menoscabar la conducción de las negociaciones y relaciones internacionales;
 - Pueda poner en riesgo la vida, seguridad o salud de una persona física;
 - Obstruya las actividades de verificación, inspección y auditoría relativas al cumplimiento de las leyes o afecte la recaudación de contribuciones;
 - Obstruya la prevención o persecución de los delitos;
 - La que contenga las opiniones, recomendaciones o puntos de vista que formen parte del proceso deliberativo de los servidores públicos, hasta en tanto no sea adoptada la decisión definitiva, la cual deberá estar documentada;
 - Obstruya los procedimientos para fincar responsabilidad a los servidores públicos, en tanto no se haya dictado la resolución administrativa;
 - Afecte los derechos del debido proceso;

- Vulnere la conducción de los expedientes judiciales o de los procedimientos administrativos seguidos en forma de juicio, en tanto no hayan causado estado;
 - Se encuentre contenida dentro de las investigaciones de hechos que la ley señale como delitos y se tramiten ante el Ministerio Público,
- Se considera **información confidencial** la que contiene datos personales concernientes a una persona identificada o identificable, entre los que se encuentran:
- Registro Federal de Contribuyentes;
 - Número de seguridad social;
 - CURP;
 - Deducciones Personales;
 - Sello digital del CFDI;
 - Sello SAT;
 - Cadena original del complemento de certificación digital del SAT.

En ese orden, los titulares de las áreas a quienes se turne la solicitud de información propuesta deberán pronunciarse sobre la existencia y clasificación de la información materia de la solicitud, así como realizar el trámite interno correspondiente a fin de proporcionar aquella que se ajuste a los dispositivos legales en comento.

TRÁMITE PARA LA ATENCIÓN DE LA SOLICITUD DE ACCESO A LA INFORMACIÓN. A efecto de garantizar el derecho humano de acceso a la información del solicitante, y para que el mismo se otorgue de manera expedita, esta Unidad de Transparencia, en términos de las facultades otorgadas por los artículo 41, fracciones II y IV, 123 de la Ley de Transparencia; mediante atento oficio, al que deberá anexarse copia cotejada de la solicitud de información pública, y del presente acuerdo, solicítese al JEFE DE LA SECCIÓN DE SOPORTE ESPECIALIZADO DE TICS, con el objeto de que realice una búsqueda exhaustiva y razonable de la información solicitada:

I. JEFE DE LA SECCIÓN DE SOPORTE ESPECIALIZADO DE TICS.

**INFORMACIÓN
SOLICITADA.**

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

2. Señalar sí 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, se han implementado las siguientes medidas: a) estándares técnicos definidos por la Coordinación de Estrategia Digital Nacional, en la contratación de bienes y servicios de seguridad de la información o de tecnologías de la información y comunicación; 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 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); 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).

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 si se emplea la firma electrónica avanzada en la institución;

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

6. Señalar si 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

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

8. 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; 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.

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

	<p>10. Informar sí la página web de la institución cuenta con: a) aviso de privacidad; b) certificados digitales vigentes;</p> <p>11. Informar sí el personal responsable se ha capacitado en la implementación del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos;</p> <p>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; b) Indicadores que permitan medir la madurez institucional en la gestión de seguridad de la información;</p> <p>13. 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 y cuántas horas de capacitación en ciberseguridad se realizan de forma anual.</p> <p>15. 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, 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 (LGPDPPO);</p> <p>17. Informar sí se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos;</p> <p>19. Informar sí han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas;</p> <p>23. Informar sí se cuenta con un plan de comunicación institucional en caso de un incidente de ciberseguridad o seguridad de la información;</p>
--	--

	<p>24. Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución;</p> <p>25. Informar sí se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad;</p> <p>26. 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. Un help desk es un equipo centralizado dentro de una empresa que atiende incidencias y reportes de sistemas informáticos y software de una organización</p> <p>27. Informar sí se cuenta con un Centro de Operaciones de Ciberseguridad Además informar si han tenido incidentes de ciberseguridad (sin importar ni decir cuáles)</p>
--	---

y proceda a dar respuesta a los puntos de la solicitud de folio **292165724000061**, especificadas en la tabla que antecede, remitiendo la información a esta Unidad de Transparencia y Protección de Datos Personales dentro del término de **5 días hábiles** contados a partir del día siguiente a la recepción del oficio de mérito, debiendo acompañar la información correspondiente, y en su caso pronunciarse sobre la existencia, inexistencia o clasificación de la información materia de la solicitud, así como realizar el trámite interno correspondiente a fin de proporcionar aquella que se ajuste a los dispositivos legales; lo anterior, a efecto de que esta Unidad de Transparencia pueda acordar lo que en derecho corresponda en relación a la respuesta que deba darse a la solicitud que nos ocupa, de conformidad con el artículo 124 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tlaxcala.

Finalmente, una vez, que el Jefe de la Sección de Soporte Especializado de TICS, haya dado cumplimiento a lo solicitado, esta Unidad al dictar acuerdo de respuesta a la solicitud, deberá pronunciarse respecto de los puntos marcados con los números 14, 16, 18, 20, 21, y 22, de la misma solicitud de información; toda vez, que es el área competente que cuenta con la información o debe tenerla de acuerdo a sus facultades, competencias y

funciones, con el objeto de que realice una búsqueda exhaustiva y razonable de la información solicitada.

II. UNIDAD DE TRANSPARENCIA Y PROTECCIÓN DE DATOS PERSONALES.

<p>INFORMACIÓN SOLICITADA.</p>	<p>14. 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?;</p> <p>16. 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, 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);</p> <p>18. 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.</p> <p>20. Informar sí se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son;</p> <p>21. 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;</p> <p>22. Informas sí se cuenta con documento de seguridad en materia de protección de datos personales;</p>
---------------------------------------	--



MEDIO PARA RECIBIR NOTIFICACIONES. Se tiene señalado como medio para que la solicitante de información pública reciba toda clase de notificaciones relativas a su solicitud, el electrónico a través del Sistema de Solicitudes de la Plataforma Nacional de Transparencia, así como en el correo electrónico cybertichr@protonmail.com.

Así lo acordó y firma el Licenciado en Derecho Marco Antonio Zelocualtecatl León, Jefe de Unidad de Transparencia y Protección de Datos Personales del Tribunal de Justicia Administrativa del Estado de Tlaxcala. **Conste.** -----



**TRIBUNAL DE JUSTICIA
ADMINISTRATIVA DEL
ESTADO DE TLAXCALA.**
UNIDAD DE TRANSPARENCIA
Y PROTECCIÓN DE DATOS PERSONALES

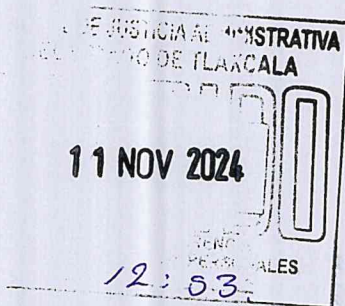
OFICIO No. TJA/DTIC/061/2024

Asunto: El que se indica

LIC. MARCO ANTONIO ZELOCUALTECATL LEÓN
JEFE DE LA UNIDAD DE TRANSPARENCIA Y
PROTECCIÓN DE DATOS PERSONALES
DEL TRIBUNAL DE JUSTICIA ADMINISTRATIVA
DEL ESTADO DE TLAXCALA
P R E S E N T E

Sirva el presente para enviarle un respetuoso saludo, En atención al oficio **TJA-UTPDP-107-2024**, donde me solicita que de acuerdo con mis atribuciones de respuesta a los puntos señalados a la solicitud de información publica con número de folio **292165724000061**, le hago entrega de un documento en Word, constante de 3 páginas las cuales contiene las respuestas a las preguntas de la solicitud antes mencionada.

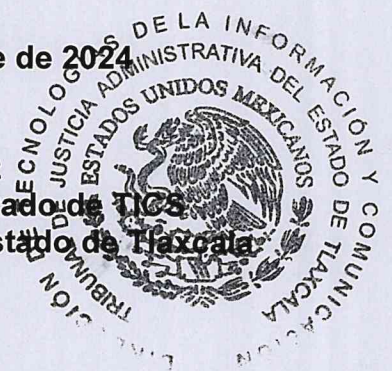
Sin otro particular y refrendando el apoyo solicitado, quedo a sus órdenes.



ATENTAMENTE

Tlaxcala, Tlaxcala; a 11 de noviembre de 2024

Ing. Julián Palma Hernández
Jefe de la Sección de Soporte Especializado de TICS
del Tribunal de Justicia Administrativa del Estado de Tlaxcala



*Anexo documento
word*

Tlaxcala de Xicohtécatl, Tlaxcala, a doce de noviembre de dos mil veinticuatro.

VISTO el contenido del oficio TJA/DTIC/061/2024, signado por el INGENIERO JULIÁN PALMA HERNÁNDEZ, en su carácter de JEFE DE LA SECCIÓN DE SOPORTE ESPECIALIZADO DE TICS DEL TRIBUNAL DE JUSTICIA ADMINISTRATIVA DEL ESTADO DE TLAXCALA; al que se anexó: **1.** Un documento Word denominado “PREGUNTAS 2024”, mismo que contiene respuestas a la solicitud de información; oficio recibido en esta Unidad de Transparencia y Protección de Datos Personales, a las doce horas con cincuenta y tres minutos, del once de noviembre de dos mil veinticuatro; **SE ACUERDA:**

CUMPLIMIENTO DE ÁREA ADMINISTRATIVA. Con fundamento en los artículos 6 de la Constitución General de la República, y 97 bis, de la Constitución Política del Estado Libre y Soberano de Tlaxcala, 1, 4, 6, 8, 16, 17, 121, 124 y 136 de la Ley General de Transparencia y Acceso a la Información Pública, 1, 4, 6, 16, 17, 24, 41 fracciones II, IV y V, 53, 116, 117, 121, 122, 123 y 124 de la Ley de Transparencia y Acceso a la Información Pública del Estado, téngase por recibido el oficio signado por el JEFE DE LA SECCIÓN DE SOPORTE ESPECIALIZADO DE TICS DEL TRIBUNAL DE JUSTICIA ADMINISTRATIVA DEL ESTADO DE TLAXCALA; a través del cual da cumplimiento a lo solicitado por esta Unidad de Transparencia en acuerdo de cinco de noviembre de dos mil veinticuatro, mismo que se ordena agregar al Expediente de Acceso a Información Pública 48/2024.

RESPUESTA A LA SOLICITUD DE INFORMACIÓN. Primero, visto el contenido del oficio TJA/DTIC/061/2024, signado por el INGENIERO JULIÁN PALMA HERNÁNDEZ, en su carácter de JEFE DE LA SECCIÓN DE SOPORTE ESPECIALIZADO DE TICS DEL TRIBUNAL DE JUSTICIA ADMINISTRATIVA DEL ESTADO DE TLAXCALA; al que se anexó: **1.** Un documento Word denominado "PREGUNTAS 2024", mismo que contiene respuestas a la solicitud de información; oficio recibido en esta Unidad de Transparencia y Protección de Datos Personales, a las doce horas con cincuenta y tres minutos, del once de noviembre de dos mil veinticuatro, se advierte que el titular del área administrativa de este sujeto Obligado, dio respuesta a la solicitud de información que le fue solicitada por esta Unidad en relación con la solicitud de acceso a la información de folio 292165724000061.

En segundo término, en cumplimiento a lo ordenado en acuerdo de cinco de noviembre del año en curso, esta Unidad de Transparencia y Protección de Datos Personales procede a dar respuesta a los puntos 14, 16, 18, 20, 21, 22, de la siguiente manera:

"

14. *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: *No se cuenta con un sistema de gestión de protección de datos personales.*

16. *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, lo anterior en términos de lo establecido por el artículo 40, 41 y 42 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO);*

Respuesta: *si, redes sociales WhatsApp y Facebook.*

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.

Respuesta: Si cuentan con conocimientos.

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

Respuesta: no, solo las que expresamente señala la Ley de la materia.

21. 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;

Respuesta: Si, la Plataforma Nacional de Transparencia, pero no se han llevado a cabo evaluaciones de impacto en materia de Protección de Datos Personales.

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

Respuesta: si, los avisos de privacidad.

Por tanto, con fundamento en el artículo 124 de la Ley de Transparencia y Acceso a la información Pública del Estado de Tlaxcala, con el contenido del oficio de cuenta y su anexo, el acuerdo de cinco de noviembre de dos mil veinticuatro, y del presente acuerdo, dese respuesta al o la solicitante de acceso a la información pública.

MEDIO DE IMPUGNACIÓN. Finalmente, atendiendo a que se ha dado respuesta a la solicitud de información, se hace saber al o la solicitante que tiene el derecho de inconformarse,

mediante recurso de revisión dentro de los quince días siguientes a la fecha de notificación del presente acuerdo, esto en términos del artículo 134 de la Ley de Transparencia y Acceso a la información Pública del Estado de Tlaxcala.

ARCHIVO. En su oportunidad archívese el presente expediente como total y definitivamente concluido.

NOTIFICACIÓN. Notifíquese el presente acuerdo al o la solicitante a través del Sistema de Solicitudes de Acceso a la Información de la Plataforma Nacional de Transparencia, así como en el correo electrónico cybertichr@protonmail.com señalado para tal efecto.

Así lo acordó y firma el Licenciado en derecho Marco Antonio Zelocualtecatl León, Jefe de la Unidad de Transparencia y Protección de Datos Personales del Tribunal de Justicia Administrativa del Estado de Tlaxcala. **Conste.** - - - - -



TRIBUNAL DE JUSTICIA
ADMINISTRATIVA DEL
ESTADO DE TLAXCALA.
UNIDAD DE TRANSPARENCIA
Y PROTECCIÓN DE DATOS PERSONALES