Oficio: UTTJA/245/2024
Solicitud: UT TJA-185-110200100018524-2024

Estimado Solicitante
PRESENTE

En atención a su solicitud de acceso a la información pública asignada bajo el folio interno **UT TJA-185-110200100018524-2024**, remitida el 30 treinta de octubre de 2024 dos mil veinticuatro, a través del sistema de solicitudes de acceso a la información de la Plataforma Nacional de Transparencia, por la que pide:

"Solicito la siguiente información

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 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 autoridad correspondiente;

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

8. 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;*
- *b) control institucional de la totalidad de los correos contenidos en las carpetas de los usuarios;*
- *c) 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;*
- *d) cuenta con cifrado en el envío de información.*

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

10. Informar sí la página web de la institución cuenta con:

- *a) aviso de privacidad;*
- *b) certificados digitales vigentes;*

11. Informar sí 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 seguirdad de la información;*
- *b) Indicadores que permitan medir el 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 artículios 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 artículios 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 sí han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas;

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

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;

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

23. Informar sí 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 sí 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 sí se cuenta con un Centro de Operaciones de Ciberseguridad Además informar si han tenido incidentes de ciberseguridad (sin importar ni decir cuáles) " ***[sic]***

Se informa:

PRIMERO. De conformidad con lo previsto por los artículos 6, letra A, fracción I, de la Constitución Política de los Estados Unidos Mexicanos y 7, fracciones VII y XII, de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Guanajuato, así como lo dispuesto por los numerales 81, de la Constitución Política para el Estado de Guanajuato; 2 y 48 de la Ley Orgánica del Tribunal de Justicia Administrativa del Estado de Guanajuato; este Tribunal es competente para atender la solicitud de acceso a la información.

SEGUNDO. Del análisis que este Tribunal de Justicia Administrativa realiza a la petición de referencia y de acuerdo con la información rendida por el área correspondiente, se le hace de su conocimiento lo siguiente:

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

R=No

2. Señalar sí 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:

R = Se operan los mecanismos establecidos en la Ley de Contrataciones Públicas del Estado de Guanajuato.

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:

R = Si, se operan los mecanismos establecidos en la Ley de Contrataciones Públicas del Estado de Guanajuato.

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

R = Si, febrero 2024.

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

R = Si, febrero 2024.

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

R = No.

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

R = No.

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:

R = No.

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

R = Se cuenta con la identificación de los activos de la institución, así como de los procesos relacionados con el área de informática.

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

R = Si, el equipo del área de informática.

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:

R = No

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

R = Se utiliza la firma electrónica del poder judicial y la firma electrónica del Estado de Guanajuato, para ciertos procesos.

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

R = No.

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, ha contado con el Dictamen Técnico favorable expedido por la autoridad correspondiente:

R = Las compras y/o contrataciones relacionadas con bienes y servicios informáticos, cuentan con el análisis de la Coordinación de Informática, respecto a su necesidad.

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

R = Propios

8. 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:

R = No existe correo electrónico institucional, se manejan algunas cuentas proporcionadas por otra institución gubernamental.

a) inserción de leyenda de confidencialidad de la información:

R = no aplica.

b) control institucional de la totalidad de los correos contenidos en las carpetas de los usuarios:

R = no aplica.

c) 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:

R = no aplica.

d) cuenta con cifrado en el envío de información:

R = no aplica.

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

R = No, sin embargo, se realizan de manera constante capacitaciones referentes al correcto tratamiento de datos personales y la importancia de la confidencialidad de la información.

10. Informar sí la página web de la institución cuenta con:

a) aviso de privacidad:

R = Si, se cuenta con un Aviso de Privacidad Integral y un Simplificado.

b) certificados digitales vigentes:

R = Si.

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

R = No.

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:

R = Si, se cuenta con mecanismos de supervisión, a través de la consola de Antivirus, para el comportamiento de los endpoints.

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

R = No

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:

R = No

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?

R = No.

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):

R = No, sin embargo, no se han registrado vulneraciones a los datos personales, toda vez que se llevan a cabo de manera continua y periódica, capacitaciones a los servidores públicos, para el correcto tratamiento de datos personales, así para la confidencialidad de la información.

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):

R = No, sin embargo, no se han registrado vulneraciones a los datos personales, toda vez que se llevan a cabo de manera continua y periódica, capacitaciones a los servidores públicos, para el correcto tratamiento de datos personales, así para la confidencialidad de la información

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

R = Si, los Lineamientos de Uso de Sistemas, Tecnologías de Información y Comunicaciones del Tribunal de Justicia Administrativa del Estado de Guanajuato, establecen disposiciones al respecto.

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:

R = Si cuentan con conocimientos en esas materias.

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

R = Si, una.

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

R = Si, la constante capacitación del personal en materia de protección de datos personales, el inicio del proceso de elaboración de avisos de privacidad, así como el inicio del proceso de elaboración del documento de seguridad de la institución y la difusión sobre la importancia de la protección de los datos personales a través de infografías y videos.

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:

R = Las plataformas digitales en la institución si realizan un tratamiento de datos personales, sin embargo, es importante mencionar, que se cuenta con un aviso de privacidad, anudado a ello, el personal está capacitado en el correcto tratamiento de los datos personales. Por lo que respecta al segundo supuesto se informa que no se han realizado estudios de impacto.

22. Informas sí se cuenta con documento de seguridad en materia de protección de datos personales:

R = No, el mismo se encuentra en proceso de elaboración.

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

R = No.

24. Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución:

R = No existe temporalidad específica.

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

R = No.

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:

R = Si, interno.

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):

R = No existe un centro de operaciones de ciberseguridad, si 1 incidente.

Lo anterior, encuentra su fundamento en lo dispuesto por los artículos 48 fracciones II, III, IV, V y VI, 82, 83, 84, 85, 88, 92, 94, 95, 96, 99, 129 y 141 de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Guanajuato.

Sin más por el momento, quedo a sus órdenes.

A T E N T A M E N T E

Silao de la Victoria, Guanajuato, a 07 siete de noviembre de 2024 dos mil veinticuatro
Titular de la Unidad de Transparencia del Tribunal de Justicia Administrativa.
Licenciado Agustín Corona Maldonado