TEJA
Tribunal Estatal de Justicia Administrativa de San Luis Potosí

05 DE NOVIEMBRE DE 2024
TAIP5-0046/2024
UNIDAD DE TRANSPARENCIA

Qt
P R E S E N T E.-

En atención a su solicitud de información registrada en el Sistema SISAI- PNT con el número de folio **240477524000046,** recibida en este Tribunal para efectos legales el día treinta de noviembre del dos mil veinticuatro, mediante la cual se formulan los siguientes requerimientos de información:

"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 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 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; 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 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 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 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)"

Me permito informarle que esta Unidad de Transparencia en atención a su solicitud de información y de conformidad con el artículo 54 fracciones IV y V de la Ley de Transparencia y Acceso a la Información Pública del Estado de San Luis Potosí, da respuesta a su solicitud en los siguientes términos:

Con respecto al cuestionario enviado consistente en veintisiete requerimientos de información, le informo que los Titulares de la Unidad de Tecnologías de la Información y la Comunicación y de la Unidad de Transparencia de acuerdo a sus funciones y atribuciones elaboraron las respuestas a sus planteamientos por lo que se adjunta dichos cuestionarios incluidos los planteamientos y sus respuestas.

Conforme a lo dispuesto en el artículo 166 de la Ley de Transparencia y Acceso a la Información Pública del Estado de San Luis Potosí; el solicitante podrá interponer, por sí mismo o a través de su representante, de manera directa o por medios electrónicos, recurso de revisión ante la Comisión Estatal de Garantía de Acceso a la Información Pública del Estado de San Luis Potosí o ante la Unidad de Transparencia que haya conocido de la solicitud dentro de los quince días siguientes a la fecha de la notificación de la respuesta, o del vencimiento del plazo su notificación.

A T E N T A M E N T E

UNIDAD DE TRANSPARENCIA DEL TRIBUNAL
ESTATAL DE JUSTICIA ADMINISTRATIVA
DE SAN LUIS POTOSI

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;

R.- No se cuenta con un gobierno de seguridad de la información, mas sin embargo se utilizan mecanismos que ayuden en la protección de la información resguardada en el Tribunal

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).

R= 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 es aplicable a la administración pública del gobierno federal de conformidad con el artículo 1 de dicho ordenamiento que señala:

> *Artículo 1.- El presente Acuerdo tiene por objeto emitir las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información, que serán de observancia obligatoria en la Administración Pública Federal. Estarán exceptuadas de su aplicación, las Secretarías de la Defensa Nacional y de Marina, así como el Centro Nacional de Inteligencia.*

Por lo anterior no le es aplicable a este sujeto obligado dicho acuerdo siendo que este Tribunal Estatal de Justicia Administrativa es un organismo autónomo y no forma parte de la Administración Pública Federal.

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 se cuenta con estrategia de ciberserguridad mas sin embargo se tienen considerados aspectos de manera que se minimicen los riesgos a vulnerabilidades.

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

R. No se emplea la firma electrónica avanzada

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

R. 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

R= 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 es aplicable a la administración pública del gobierno federal de conformidad con el artículo 1 de dicho ordenamiento que señala:

Artículo 1.- El presente Acuerdo tiene por objeto emitir las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información, que serán de observancia obligatoria en la Administración Pública Federal. Estarán exceptuadas de su aplicación, las Secretarías de la Defensa Nacional y de Marina, así como el Centro Nacional de Inteligencia.

Por lo anterior no le es aplicable a este sujeto obligado dicho acuerdo siendo que este Tribunal Estatal de Justicia Administrativa es un organismo autónomo y no forma parte de la Administración Pública Federal.

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

R. Se cuentan con centros de datos tanto propios como de terceros.

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; 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 institucional

a) No se cuenta

c) Directo con el proveedor

d) Directo con el proveedor

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. La divulgación no autorizada de la información sustantiva de este sujeto obligado cuenta con restricciones legales previstas en diversa normatividad como lo es el Código Procesal Administrativo, La Ley de Transparencia y Acceso a la Información Pública de San Luis Potosí respecto a aquella información de procedimientos seguidos en forma de juicios en tanto no se dicte sentencia cause estado y ejecutoria, La Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados que prohíbe la difusión de los datos personales la vulneración al uso de la información puede ser motivo de procedimiento de responsabilidad administrativa mecanismo que inhibe la divulgación de la información no autorizada.

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

R. Si se cuenta con avisos de privacidad en la sección de transparencia y cuenta con sus certificados SSL vigentes

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

R. El personal ha asistido a cursos y conferencias en temas de Ciberseguridad

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 el madurez institucional en la gestión de seguridad de la información;

R. No se cuenta

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 se cuenta, más sin embargo se imparten recomendaciones para mitigar riesgos de pérdida de información

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. Está en etapa de desarrollo el sistema de gestión de protección de datos personales el cual involucra a todas las áreas de este sujeto obligado y en tanto no esté terminado y autorizado por el Comité de Transparencia no se puede difundir información al respecto.

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 se cuenta con un modelo o sistema de comunicación, ya que se procedería conforme a lo establecido en el artículo 56 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de San Luis Potosí que señala:

> ARTÍCULO 56. El responsable deberá informar sin dilación alguna al titular y a la CEGAIP las vulneraciones de seguridad ocurridas, que de forma significativa afecten los derechos patrimoniales o morales del titular, en un plazo máximo de setenta y dos horas en cuanto se confirmen, y haya empezado a tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, a fin de que los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos.

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 se cuenta con un modelo o sistema de comunicación, ya que se procedería conforme a lo establecido en el artículo 56 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de San Luis Potosí que señala:

> *ARTÍCULO 56. El responsable deberá informar sin dilación alguna al titular y a la CEGAIP las vulneraciones de seguridad ocurridas, que de forma significativa afecten los derechos patrimoniales o morales del titular, en un plazo máximo de setenta y dos horas en cuanto se confirmen, y haya empezado a tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, a fin de que los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos.*

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. No se cuenta

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 experiencia comprobable en dichos temas.

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

R. No se han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la solicitud de información.

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

R. En la elaboración de Versiones Publicas se adoptó un sistema interno para proteger los datos personales así como se fomentó el uso del TEST DATA avalado por el Sistema Nacional de Transparencia.

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. En la elaboración de Versiones Publicas de las Sentencias y no se han realizado recomendaciones por parte del INAI.

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

R. Está en etapa de desarrollo el sistema de gestión de protección de datos personales y el documento de seguridad, el cual involucra a todas las áreas de este sujeto obligado y en tanto no esté terminado y autorizado por el Comité de Transparencia no se puede difundir información al respecto.

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 se cuenta

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

R. Diariamente la Unidad de Tecnologías de la Información se mantiene actualizada ante posibles vulnerabilidades cibernéticas

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

R. No se realizan

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. No se cuenta, mas sin embargo se atienden de manera oportuna cualquier incidencia

27. Informar sí se cuenta con un Centro de Operaciones de Ciberseguridad

R. No se cuenta con un Centro de Operaciones de Ciberseguridad

Además informar si han tenido incidentes de ciberseguridad (sin importar ni decir cuáles)

R. No se han tenido incidentes de ciberseguridad desde el año 2015 a la fecha de la solicitud de información.