Saltillo, Coahuila de Zaragoza a 12 de noviembre de 2024
Oficio n° STT/511/2024
Número de Folio 051259000027524

Solicitante
Presente.

Por este conducto le comunico que fue recibida por vía electrónica su petición con el número de folio 051259000027524, donde solicita:

"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; 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 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)

En mérito de lo anterior, de conformidad con los artículos 97, 99, 102 y 103 de la Ley de Acceso a la Información Pública para el Estado de Coahuila y para dar atención y respuesta a la misma, fue turnada por la Unidad de Atención a las Solicitudes de Acceso a la Información de la Secretaría Técnica y de Transparencia a la Dirección de Informática de la Oficialía Mayor del Poder Judicial.

En virtud de lo anterior, se le informa por conducto de esta Unidad, después de una búsqueda exhaustiva de la información, 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;
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; 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).
a) No.
b) Sí.
c) No.
d) No.
e) No.

f) No.
g) No.
h) Sí.
i) No.

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 ;
Sí. i) 01/06/2024 ii) 15/06/2024 iii) No se ha modificado desde su creación iv) Dirección de Innovación y Dirección de Informática.

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

5. Informar sí se realizan simulacros sobre el plan de recuperación de desastres o en caso de incidentes cibernéticos;
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, de ha contado con el Dictamen Técnico favorable expedido por la autoridad correspondiente;
No.

7. Informar sí los servicios de centros de datos son propios, de otra institución gubernamental o de un tercero;
Hay centros de datos propios de la institución, así 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.
Sí. a) No, c) Sí, d) Sí, e) Sí.

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

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

11. Informar sí el personal responsable se ha capacitado en la implementación del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos;
No.

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;
a) No, b) 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.
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?;
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 artículios 40, 41 y 42 de la Ley general de protección de datos personales en posesión de sujetos obligados (LGPDPPSO);
No.

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);
No.

17. Informar sí se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos;
No. Los usuarios no usan dispositivos móviles.

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.
Sí.

19. Informar sí han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas;
No.

20. Informar sí se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son;
Sí, los esquemas de mejores prácticas en materia de protección de datos personales adoptados son la capacitación frecuente, monitoreo periódico de los servidores y de las redes, respaldos frecuentes, aplicación de actualizaciones y uso de antivirus.

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;
Sí, no se han llevado a cabo evaluaciones de impacto en materia de protección de datos personales, ni emitido recomendación por el INAI.

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

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

24. Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución;
Dependiendo de las características técnicas se hace la revisión y actualización inmediata. Además, cada seis meses se hace una revisión exhaustiva.

25. Informar sí se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad;
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
Se tiene un sistema de Tickets de Soporte Técnico. Es para uso interno solamente.

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)
No.

Se informa lo anterior, con fundamento en lo establecido por el artículo 102 y 103 de la Ley de Acceso a la Información Pública para el Estado de Coahuila de Zaragoza, disposiciones que establecen:

> ***Artículo 102****.-La obligación de dar acceso a la información se tendrá por cumplida cuando la información se entregue al solicitante en medios electrónicos, ésta se ponga a su disposición para consulta en el sitio en que se encuentra, o bien mediante la expedición de copias simples o certificadas. El acceso a la información se dará solamente en la forma en que lo permita el documento de que se trate.*
>
> *En el caso de que la información ya esté disponible en medios electrónicos, la Unidad de Transparencia se lo indicará al solicitante, precisando la dirección electrónica completa del sitio donde se encuentra, y en la medida de sus posibilidades, podrá adjuntar a la respuesta la imagen digital que compruebe que ahí se encuentran los datos o documentos solicitados y proporcionar una impresión de la misma.*
>
> *En el caso de que la información solicitada ya esté disponible al público en medios impresos, tales como libros, compendios, informes, trípticos o en cualquier otro medio, se le hará saber al solicitante por escrito la fuente, el lugar y la forma en que puede consultar, reproducir o adquirir dicha información en un plazo no mayor a cinco días.*

> ***Artículo 103.-*** *Los sujetos obligados entregarán documentos que se encuentren en sus archivos. La obligación de proporcionar información no comprende el procesamiento de la misma, ni el presentarla conforme al interés particular del solicitante. Sin perjuicio de lo anterior, los sujetos obligados deberán sistematizar la información.*

Ello encuentra su refuerzo en el criterio SO/03/2017 emitido por el INAI y que señala:

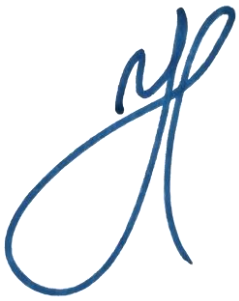
> ***No existe obligación de elaborar documentos ad hoc para atender las solicitudes de acceso a la información****. Los artículos 129 de la Ley General de Transparencia y Acceso a la Información Pública y 130, párrafo cuarto, de la Ley Federal de Transparencia y Acceso a la Información Pública, señalan que los sujetos obligados deberán otorgar acceso a los documentos que se encuentren en sus archivos o que estén obligados a documentar, de acuerdo con sus facultades, competencias o funciones, conforme a las características físicas de la información o del lugar donde se encuentre. Por lo anterior, los sujetos obligados deben garantizar el derecho de acceso a la información del particular, proporcionando la información con la que cuentan en el formato en que la misma obre en sus archivos; sin necesidad de elaborar documentos ad hoc para atender las solicitudes de información.*

Con lo anterior se responde a su solicitud de información de conformidad con lo dispuesto en los artículos 6o de la Constitución Política de los Estados Unidos Mexicanos; 7o, párrafo séptimo y 8o, párrafo sexto, de la Constitución Política del Estado de Coahuila de Zaragoza y, 97 de la Ley de Acceso a la Información Pública para el Estado de Coahuila de Zaragoza.

Por otro lado, y en cumplimiento de lo previsto por los artículos 110 y 111 de la Ley de Acceso de Información Pública para el Estado de Coahuila de Zaragoza, le comunico que si Usted no está conforme
con esta respuesta podrá presentar recurso de revisión e interponerlo de manera directa o por medios electrónicos, a través de la Plataforma Nacional de Transparencia, ante el Instituto Coahuilense de Acceso a la Información Pública.

Sin otro particular, le reitero las seguridades de mi atenta y distinguida consideración.

Atentamente



PODER JUDICIAL
DEL ESTADO DE COAHUILA DE ZARAGOZA
Unidad de Atención a las Solicitudes de Acceso a la Información de la Secretaría Técnica y de Transparencia

Yesenia Yazmín Perales Ortega
Unidad de Atención a Solicitudes de Acceso a la Información de la Secretaría Técnica y de Transparencia de la Presidencia del Tribunal Superior de Justicia del Estado.

c.c.p. Mtro. Miguel Felipe Mery Ayup. Magistrado Presidente del Tribunal Superior de Justicia del Estado de Coahuila de Zaragoza.
c.c.p. Mtro. Rodrigo González Morales. Secretario Técnico y de Transparencia de la Presidencia del Tribunal Superior de Justicia del Estado.
c.c.p. Archivo.