



Saltillo, Coahuila A 31 de Octubre de 2024
INFO/419/2024.

C. QT
PRESENTE.-

En atención a su solicitud de información recibida a través de la Plataforma Nacional de Transparencia, identificada con el número de folio 0501033000041924, a través de la cual solicita:

"...Solicito la siguiente información 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 si 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 si 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 si 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 si se cuenta con una política general de seguridad de la información y en su caso, quienes intervienen y desde cuándo se implementó; h) informar si se cuenta con un diagnóstico de identificación de los procesos y activos esenciales de la Institución; i) Informar si se cuenta con un Equipo de Respuesta a Incidentes de Seguridad de la Información (ERISC). 3. Informar si 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) si 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 autoridad correspondiente; 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 el madurez institucional en la gestión de seguridad de la información; 13. Informar si dentro de la institución se cuenta con un Programa de formación en la cultura de la seguridad de la información o de ciberseguridad; y en caso afirmativo señalar: cuándo se implementó y cuántas horas de capacitación en ciberseguridad se realizan de forma anual. 14. Informar si de conformidad con la Ley General de Protección de Datos Personales en Posesión de Sujetos obligados se cuenta con un sistema de gestión de protección de datos personales, en caso de ser afirmativa esta pregunta, ¿desde cuándo se adoptó y cuáles áreas participaron en su desarrollo e implementación?; 15. Informar si se cuenta con un modelo o sistema de comunicación, para informar a la sociedad en general sobre los eventos o incidentes de seguridad de la institución, y en caso de ser afirmativo, ¿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 si se cuenta con un modelo o sistema de comunicación para informar a los titulares de datos personales en caso de brechas de seguridad de esta información, y señalar cuáles áreas de la organización participan en su implementación y desde cuándo se implementó, o anterior en términos de lo establecido por el artículos 40, 41 y 42 de la Ley general de protección de datos personales en posesión de sujetos obligados (LGPDPPSO); 17. Informar si se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos; 18. Informar si las personas encargadas de sistemas de información, donde se brinde información pública, cuentan con conocimientos comprobables en las siguientes materias (i) transparencia; (ii) protección de datos personales; (iii) archivos públicos; o, (iv) seguridad de la información. 19. Informar si han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas; 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

**Unidad de Acceso a la Información
del Municipio de Saltillo**

Blvd. Francisco Coss 745 Zona Centro
Saltillo, Coahuila.
Tel 844 4382539
transparenciasalttillo.mx



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) ..."(sic)

Con fundamento en el artículo 95 Ley de Acceso a la Información Pública para el Estado de Coahuila de Zaragoza, hago de su conocimiento que este Sujeto Obligado no es competente para responder su solicitud de información.

Sin embargo, en aras de la transparencia, le informo que como lo señala el artículo 6 fracción V de la Ley de Acceso a la Información Pública para el Estado de Coahuila de Zaragoza, en correlación con el numeral III del Reglamento de la Administración Pública Municipal de Saltillo, Coahuila de Zaragoza, el Sujeto Obligado competente es la Comisaría de Seguridad y Protección Ciudadana, la cual es una institución de seguridad de orden municipal, cuyas facultades y atribuciones indicadas en el acuerdo de creación, adicionales a las señaladas en la Constitución Política de los Estados Unidos Mexicanos, la Constitución Política del Estado de Coahuila, el Código Municipal para el Estado de Coahuila de Zaragoza y demás ordenamientos legales aplicables son, entre otras, la de vigilar el cumplimiento y observancia de las leyes, reglamentos y disposiciones en materia de seguridad pública.

Por lo anterior, se le sugiere dirigir su petición a dicho Organismo Público Descentralizado, a través de la Plataforma Nacional de Transparencia, en el siguiente link: <http://www.plataformadetransparencia.org.mx/web/guest/inicio>. Así mismo, le proporciono su página web de transparencia: <https://saltillo.gob.mx/web/transparencia-cs/>.

Con fundamento en el artículo 110 y III de la Ley de Acceso a la Información Pública para el Estado de Coahuila de Zaragoza, si usted no está conforme, cuenta con veinte días contados a partir de la notificación de esta respuesta para interponer recurso de revisión mediante la Plataforma Nacional de Transparencia, en esta Unidad de Acceso a la Información ubicada en Francisco Coss # 745 Zona Centro Saltillo, Coahuila 25000 o acudir al propio Instituto Coahuilense de Acceso a la Información con domicilio en Allende y Manuel Acuña Edificio Pharmakon Ramos Arizpe, Coahuila, México C.P. 25900.

**GRACIAS POR EJERCER SU DERECHO A LA INFORMACIÓN.
A T E N T A M E N T E**

M.D. FRANCIA FUENTES DE LA FUENTE.
TITULAR DE LA UNIDAD DE ACCESO A LA INFORMACIÓN
DEL MUNICIPIO DE SALTILLO, COAHUILA DE ZARAGOZA