

Saltillo, Coahuila de Zaragoza, a 31 de octubre de 2024
Oficio Interno No. DEII/063/2024
Asunto: Respuesta a solicitud de información UTTAI/633/2024
Folio 051143000025424

Licda. Erika Georgina Oyervides González
Titular de la Unidad Técnica de Transparencia y
Acceso a la información Pública
Presente.-

Por este conducto, en mi carácter de Titular de la Dirección Ejecutiva de Innovación e Informática de este Instituto, en relación al oficio interno UTTAI/633/2024 con folio 051143000025424 de fecha veintiuno (21) de octubre de dos mil veinticuatro (2024), donde se solicita información referente a lo siguiente:

SECCION 1 1. Informar si dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan; 2. Señalar si cuenta con lo siguiente: b) Informar si se cuenta con un 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) o Sistema de Gestión de Seguridad de la información (SGSI); 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 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) O Equipo de respuesta a Incidentes Cibernéticos o en su caso SOC. 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 se cuentan con lineamientos de programación y desarrollo de sistemas informáticos seguros; 7. Informar si los servicios de centros de datos son propios, de otra institución gubernamental o de un tercero; 8. Informar si para el trabajo remoto se cuentan con lineamientos de seguridad para las videollamadas; 9. 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 o en su caso de transparencia y acceso a 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. 11. Informar si la página web de la institución cuenta con: a) aviso de privacidad; b) certificados digitales vigentes; 12. Informar si el personal responsable se ha capacitado en la implementación del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos; 13. Informar si se cuentan con: a) Los mecanismos de supervisión y Blvd. Luis Donaldo Colosio No. 6207, Fracc. Rancho La Torrecilla, C.P. 25298 Saltillo, Coahuila. Tel (844) 438 6260 "2024 Bicentenario de Coahuila; 200 años de grandeza" 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; 14. 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".

En relación a su petición de información acerca de la seguridad informática y ciberseguridad en nuestra institución, me permito responder lo siguiente:

1. **Gobierno de seguridad de la información o ciberseguridad:** No se ha establecido un marco formal en esta área.
2.
 - b) **Inventario institucional de bienes y servicios de TIC:** Actualmente no disponemos de un inventario sistematizado.
 - c) **Plan de continuidad de operaciones:** No existe un plan formalmente implementado.
 - d) **Plan de recuperación ante desastres:** No hemos desarrollado ni implementado un plan específico.
 - e) **Programa de gestión de vulnerabilidades:** Actualmente no contamos con un programa en este sentido.
 - f) **Marco de Gestión de Seguridad de la Información (MGSI) o Sistema de Gestión de Seguridad de la Información (SGSI):** No se ha desarrollado un marco formal.
 - g) **Política general de seguridad de la información:** En este momento, no existe una política implementada.
 - h) **Diagnóstico de identificación de procesos y activos esenciales:** No se ha llevado a cabo un diagnóstico.
 - i) **Equipo de Respuesta a Incidentes de Seguridad de la Información (ERISC):** No contamos con un equipo designado.
3. **Estrategia de ciberseguridad:** No hemos desarrollado una estrategia formal.
4. **Uso de firma electrónica avanzada:** No se está utilizando esta tecnología actualmente.
5. **Simulacros sobre el plan de recuperación de desastres:** No hemos realizado simulacros.
6. **Lineamientos de programación y desarrollo de sistemas informáticos seguros:** No se han establecido lineamientos.
7. **Servicios de centros de datos:** No contamos con servicios propios ni tercerizados.
8. **Lineamientos de seguridad para trabajo remoto:** No se han definido lineamientos específicos.
9. **Correo electrónico institucional:** Sí, contamos con un sistema de correo electrónico institucional.
 - a) **Inserción de leyenda de confidencialidad:** Sí, se incluye una leyenda de confidencialidad en los correos enviados.
 - c) **Control institucional de las carpetas de los usuarios:** No se tiene control institucional sobre los correos contenidos en las carpetas de los usuarios.
 - d) **Soluciones de filtrado para correo no deseado:** Si se cuenta con filtrado para correo no deseado.

e) **Cifrado en el envío de información:** Si se cuenta con cifrado en el envío de información.

11. **Página web institucional:**

- a) Sí, se posee.
- b) Sí, se disponen de ellos.

12. **Capacitación en el Protocolo Nacional Homologado:** No hemos llevado a cabo esta capacitación.

13. **Mecanismos de supervisión y evaluación:** Actualmente no contamos con indicadores establecidos.


14. **Programa de formación en la cultura de la seguridad:** No contamos con este programa.

En virtud de lo anterior, se da por cumplimiento a la solicitud de acceso a la información mencionada al inicio, en conformidad con lo establecido en los artículos 8, fracción III, y 99 de la Ley de Acceso a la Información Pública para el Estado de Coahuila de Zaragoza.

Sin otro particular, me reitero a su disposición para cualquier consulta o aclaración que requiera.



Atentamente


Ing. Jorge Gallegos Valdés
Director Ejecutivo de Innovación e Informática



IEC
Instituto Electoral de Coahuila

C.c.p.: Archivo.

Aprobó		
Revisó	Jorge Gallegos Valdés	
Elaboró	Adriana Dávora Serna	