SINALOA
TRIBUNAL ELECTORAL

UNIDAD DE TRANSPARENCIA
No DE FOLIO: 251159300004124

C. SOLICITANTE

PRESENTE.-

En relación con su solicitud de información, realizada a este órgano jurisdiccional, a través del Sistema de Solicitudes de Acceso a la Información de la Plataforma Nacional de Transparencia con número de folio 251159300004124 con fecha de impresión del acuse 22 de octubre del 2024, en el que 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 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 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;

SINALOA
TRIBUNAL ELECTORAL

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)."

Al respecto, me permito dar respuesta, en términos de la información proporcionada por el área competente, Unidad de Comunicación, la cual se anexa al presente.

Lo anterior de conformidad con los artículos 1, 2, 19, 68, 135 y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Sinaloa.

Reciba un cordial saludo.

A T E N T A M E N T E

Culiacán, Sin., 13 de noviembre de 2024.

MTRA. ANABEL IBÁÑEZ ÁLVAREZ

ENCARGADA DE LA UNIDAD DE TRANSPARENCIA

C..c.p. Archivo

SINALOA
TRIBUNAL ELECTORAL

Culiacán, Sinaloa, 13 de noviembre de 2024
Oficio No. 02/2024

Mtra. Anabel Ibañez Alvarez
Encargada de la Unidad de Transparencia
Presente.-

Por medio del presente y en atención al oficio TEESIN/UT/ 049/2024, el cual hace referencia a la solicitud de información registrada en la Plataforma Nacional de transparencia, de fecha 30 de octubre del 2024 con número de folio 251159300004124, mediante la cual se solicita la siguiente información:

Con relación a la solicitud de información relacionada con temas de ciberseguridad, en primer término, debe precisarse que, el Tribunal es un organismo constitucional autónomo cuya principal función es la jurisdiccional, es decir, la resolución de medios de impugnación en materia electoral. Al ser una institución especializada en la materia, destina principalmente su presupuesto a personal especializado en la resolución de estos asuntos (82.66%); pues de la totalidad de su personal, el 62% tiene atribuciones de naturaleza jurisdiccional, y solo el 38% de naturaleza administrativa u otras.

De ahí que, este Tribunal no cuente con un área especializada en sistemas de la información o informáticos, sino que, estos servicios son contratados a un proveedor externo a las areas de funcionamiento del Tribunal, teniendo como enlace de estos servicios a la Unidad de Comunicación; sin embargo, de acuerdo a las necesidades de la institución, dicha Unidad no requiere un perfil específico en materia de ciberseguridad.

Respecto a la seguridad de los equipos de cómputo asignados al personal de este Tribunal, únicamente se cuenta con la seguridad de antivirus en cada uno de ellos.

Una vez precisado lo anterior, a continuación, se dará respuesta a los puntos que contiene la solicitud de información.

1. Informar si dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan.
Respuesta: Este Tribunal no cuenta con un gobierno de seguridad o ciberseguridad.

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).
Respuesta: Este Tribunal no cuenta con la Ciberseguridad en materia de Tecnologías de la Información ni con ninguno de los documentos indicados en los incisos señalados.

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;
Respuesta: Este Tribunal no cuenta con una estrategia de Ciberseguridad.

4. Informar si se emplea la firma electrónica avanzada en la institución;
Respuesta: Este Tribunal no cuenta ni emplea la firma electrónica avanzada.

5. Informar si se realizan simulacros sobre el plan de recuperación de desastres o en caso de incidentes cibernéticos;
Respuesta: Este Tribunal no realiza simulacros sobre un plan de incidentes ciberneticos.

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
Respuesta: Este tribunal no ha contratado servicios de seguridad de la información arriba mencionados.

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

Respuesta: Este tribunal no tiene un servidor de centros de datos para almacenar la información, cada área realiza el guardado de información en el equipo de cómputo asignado.

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 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.

Respuesta: Este Tribunal no inserta una leyenda de confidencialidad de la información en los correos electrónicos; sí tiene el control de cada usuario de la totalidad de sus correos electrónicos institucionales; sí utiliza el filtrado de correo no deseado dentro del correo utilizado y el mismo proporcional, mientras que no se cuenta con el cifrado de envío de información.

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

Respuesta: Este Tribunal no cuenta con mecanismos para evitar la divulgación no autorizada de datos.

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

a) aviso de privacidad;

b) certificados digitales vigentes;

Respuesta: La página de este tribunal si cuenta con aviso de privacidad y nuestra página cuenta con 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;

Respuesta: El personal no ha sido capacitado en esta materia.

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;

Respuesta: Este Tribunal no cuenta con controles de seguridad de la información ni con controles de ciberseguridad, de ahí que se cuente con mecanismos de supervisión y evaluación de los mismos.

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 cuántas horas de capacitación en ciberseguridad se realizan de forma anual.
Respuesta: Este tribunal no cuenta con un programa de formación en cultura de seguridad de la información o ciberseguridad.

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?;
Respuesta: Este tribunal no cuenta con un sistema de gestión de protección de datos personales.

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 artículios 40, 41 y 42 de la Ley general de protección de datos personales en posesión de sujetos obligados (LGPDPPSO);
Respuesta: Este tribunal no cuenta con un modelo o sistema específico de comunicación para informar de incidentes de esta naturaleza.

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 artículios 40, 41 y 42 de la Ley general de protección de datos personales en posesión de sujetos obligados (LGPDPPSO);
Respuesta: Este tribunal no cuenta con un modelo o sistema de comunicación para informar a los titulares de datos personales en caso de brechas de seguridad.

17. Informar si se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos;
Respuesta: Este tribunal no cuenta con lineamientos para el traslado de activos fisicos (dispositivos móviles).

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.
Respuesta: Este Tribunal no cuenta con un área de Sistemas de información con conocimientos en las materias mencionadas.

19. Informar si han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas;
Respuesta: Este Tribunal nunca ha tenido problemas de ciberseguridad ni pérdida de información desde la fecha indicada.

20. Informar si se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son;
Respuesta: Este Tribunal no ha adoptado esquemas de mejores práticas en materia de protección de datos personales.

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;
Respuesta: Este Tribunal no tiene plataforma, aplicación u otra tecnología para el tratamiento intensivo y/o relevante de datos personales.

22. Informar si se cuenta con documento de seguridad en materia de protección de datos personales;
Respuesta: Este Tribunal no cuenta con documento de seguridad en materia de datos personales.

23. Informar si se cuenta con un plan de comunicación institucional en caso de un incidente de ciberseguridad o seguridad de la información;
Respuesta: Este tribunal no cuenta con un plan de comunicación institucional para ciberseguridad o seguridad de la información.

24. Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución;
Respuesta: Este Tribunal al no contar con un área de sistemas, no cuenta y por ende, no actualiza 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;
Respuesta: Este Tribunal no ha llevado a cabo auditorías externas o internas en la materia.

27. 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
Respuesta: Este Tribunal no cuenta con help desk.

33. Informar sí se cuenta con un Centro de Operaciones de Ciberseguridad Además informar si han tenido incidentes de ciberseguridad (sin importar ni decir cuáles)
Respuesta: Este Tribunal no cuenta con un centro de operaciones de ciberseguridad, tampoco ha habido incidentes de ciberseguridad.

Ismael Martínez Partida
Titular de la Unidad de Comunicación