EXPEDIENTE: TJA-UT-052/2024
FOLIO: 270511700005224
ACUERDO: Disponibilidad.

Cuenta: Con la Solicitud de Acceso a Información Pública, folio número **270511700005224,** de fecha ***treinta de octubre de dos mil veinticuatro*** y el oficio ***TJA-DAI/014-2024***, de fecha ***siete de noviembre de dos mil veinticuatro***, se procede a emitir el correspondiente acuerdo: Conste. -

TRIBUNAL DE JUSTICIA ADMINISTRATIVA DEL ESTADO DE TABASCO, UNIDAD DE TRANSPARENCIA Y EQUIDAD DE GÉNERO; VILLAHERMOSA, TABASCO, A OCHO DE NOVIEMBRE DE DOS MIL VEINTICUATRO. -

Visto: Con fundamento en los artículos 47, 49, 50 fracciones III y VI, 131, 133, y 138 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco, se **ACUERDA:** -

PRIMERO. Vía electrónica Plataforma Nacional de Transparencia, él ***treinta y uno de octubre del año en curso***, se recibió la solicitud de información Pública con número de folio ***270511700005224***, de fecha **treinta *de octubre de dos mil veinticuatro***, bajo los siguientes términos: -

APARTADO 1
1. Informar sí dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan;
2. Señalar sí se cuenta con lo siguiente: a) un marco de 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) o Sistema de Gestión de Seguridad de la Información (SGSI); 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) o Equipo de respuesta a Incidentes Cibernéticos o en su caso SOC.

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 si se cuentan con lineamientos de programación y desarrollo de sistemas informáticos seguros;

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

8. Informar sí para el trabajo remoto se cuentan con lineamientos de seguridad para las videollamadas;

9. 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 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.

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

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

12. Informar sí 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 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 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

15. 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?;

16. 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;

17. 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;

18. Informar sí se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos;

19. 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.
20. Informar sí han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas;
21. Informar sí se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son;
22. 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;
23. Informas sí se cuenta con documento de seguridad en materia de protección de datos personales;
24. Informar sí se cuenta con un plan de comunicación institucional en caso de un incidente de ciberseguridad o seguridad de la información;
25. Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución;
26. Informar sí se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad;
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.
28. Señalar sí las páginas web de los buscadores de versiones públicas de sentencias del Tribunal, tienen certificados digitales vigentes.
APARTADO 2
Solicito la siguiente información.
29. Informar sí dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan;
30. 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 ;
31. Informar sí se cuenta con un sistema de gestión de seguridad de la información dentro de la institución;
32. Informar sí de conformidad con la Ley General de Protección de Datos Personales en Posesión de Particulares se cuenta con lo siguiente 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?;
33. Informar sí es que se cuenta con un plan de continuidad del negocio, para el caso de algún evento o incidente de seguridad cibernética o física". Sic

SEGUNDO. Con fundamento en los artículos 49, 50, fracción III y 138 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco, siendo de la competencia de este Tribunal de Justicia Administrativa, en su calidad de Sujeto Obligado, conocer y resolver, por cuanto a la solicitud de información presentada vía electrónica, se turnó a las áreas correspondientes que fungen como enlaces de Transparencia del Tribunal de Justicia Administrativa del Estado de Tabasco, los oficios correspondientes, para que de acuerdo a sus atribuciones y competencia, dieran respuesta a lo peticionado. Documentos que se adjuntan al presente acuerdo para los efectos leales a que haya lugar. --

TERCERO. Hágasele saber a la interesada, que de conformidad con los artículos 148, 149 y 150 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco, puede interponer por sí mismo o a través de representante legal, recurso de revisión dentro de los quince días hábiles siguientes a la notificación del presente acuerdo, ante el Instituto Tabasqueño de Transparencia y Acceso a la Información Pública, en caso de no estar conforme. -

CUARTO. En términos de los artículos 50, 132, 138 y 139 de la Ley de la materia. Notifíquese a través de la Plataforma Nacional de Transparencia, para los efectos legales conducentes. -

Así lo acordó, manda y firma, ***MDC. Tila del Carmen De la Rosa Jiménez, Titular de la Unidad de Transparencia y Equidad de Género,*** del Tribunal de Justicia Administrativa del Estado de Tabasco, quien legalmente actúa y da fe. -

TRIBUNAL DE JUSTICIA ADMINISTRATIVA
DEL ESTADO DE TABASCO

I.S.C. MARCOS URIEL MONTUY SANSORES
Titular de la Unidad de Archivo e Informática

Asunto: RESPONDIENDO OFICIO TJA-UT-129/2024
Oficio: TJA/DAI/014-2024
Fecha: 07/11/2024

TRIBUNAL DE JUSTICIA ADMINISTRATIVA DEL ESTADO DE TABASCO
RECIBIDO
07 NOV 2024
12:30 hrs
UNIDAD DE TRANSPARENCIA

M.D.C. TILA DEL CARMEN DE LA ROSA JIMÉNEZ
TITULAR DE LA UNIDAD DE TRANSPARENCIA
Y EQUIDAD DE GENERO DEL TRIBUNAL DE
JUSTICIA ADMINISTRATIVA DEL ESTADO DE
TABASCO.

Es grato dirigirme a usted, en atención a su oficio: TJA-UT-129/2024, respecto a la solicitud de acceso a la información de folio: 270511700005224, de fecha 31 de octubre de 2024, desglosando la respuesta de la misma de la forma siguiente:

APARTADO 1

1. Informar sí dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan;

R.- En este Tribunal de Justicia Administrativa del Estado de Tabasco (TJA), se trabaja con salida a internet, la cual está limitada en velocidad y administrada por un firewall, mismo que administra salidas y bloquea entradas a todos los puertos en todas las áreas, incluido los del server, una de las razones por la cual no se trabaja VPN.

2. Señalar sí se cuenta con lo siguiente:

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.

R.- De momento no contados con los estándares mencionados, debido a que no se cuenta con el presupuesto necesario para la contratación de bienes y servicios de seguridad de la información.

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;

R.- Se cuenta con un inventario de los Bienes y servicios, pero al no contar con un comité de TIC no se cuenta con un proceso realizado por el mismo.

c) un plan de continuidad de operaciones, y señalar la fecha de implementación;

R.- Se cuenta con un programa para continuidad, implementado a partir del mes de mayo del 2022.

d) Informar sí se ha desarrollado e implementado el plan de recuperación ante desastres, señalar la fecha de desarrollo e implementación;

R.- Se desarrolló un plan de recuperación en caso de desastres, a partir del mes de mayo de 2022.

e) desarrollado e implementado un programa de gestión de vulnerabilidades;

R.- No se ha desarrollado, se aplica cuidados continuos en el manejo de los equipos de información.

f) Marco de Gestión de Seguridad de la Información (MGSI) o Sistema de Gestión de Seguridad de la Información (SGSI);

R.- No se cuenta con el mismo.

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;

R.- Se aplica una política en el manejo de la información, implementada desde los inicios de labores del Tribunal, en la cual participan activamente todas las áreas.

h) informar sí se cuenta con un diagnóstico de identificación de los procesos y activos esenciales de la Institución;

R.- Se tienen identificados los procesos y activos pero no se cuenta con un diagnostico plasmado como tal.

i) Informar sí se cuenta con un Equipo de Respuesta a Incidentes de Seguridad de la Información (ERISC.

R.- Por cuestiones presupuestales no se cuenta con un equipo de respuesta a incidentes de seguridad de la información.

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.- Se aplican políticas de seguridad en el manejo de la información del TJA, pero no se cuenta con una estrategia plasmada mediante un programa establecido.

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

R.- En estos momentos todavía no se aplica la firma electrónica, estamos en estudios y análisis para su implementación.

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

R.- Por cuestiones de tiempo y la carga de trabajo, no se realizan simulacros, sin embargo se aplican las políticas de respaldo de información.

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.- No se cuenta con los dictámenes técnicos favorables debido a que no se ha realizado ningún contratación de servicios de seguridad en la información, por motivos presupuestales.

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

R.- En este TJA los servicios son propios, manejados y administrados por cada área.

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 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.

R.- Se cuenta con un correo electrónico institucional, mismo que es asignado por una empresa que proporciona hospedaje web e incluye cuentas de correo, el cual garantiza los controles de seguridad, respaldo, no deseados, etc. necesarios, dentro de los cuales se incluyen la leyenda correspondiente al área y que están administrados institucionalmente.

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.- Se cuenta con políticas administrativas para el manejo de la información en cuando a la divulgación de datos se refiere.

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

R.- Se cuenta con avisos de privacidad y certificados digitales funcionales.

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

R.- No se ha llevado capacitación.

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 con ello, estamos en proceso de análisis, para implementación.

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.

R.- No se cuenta con el Programa, estamos en proceso de análisis, para implementación.

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.- No se cuenta con un sistema pero si con políticas de acuerdo a la Ley General de Protección de Datos Personales en Posesión de Sujetos obligados.

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 sistema como tal, se informa a través de la página web y medios impresos en caso de ocurrir, mismo que no ha sido necesario.

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);

R.- No se cuenta con un sistema digital, en caso de ocurrir se realiza mediante oficios enviados a los enlaces por medio de correo electrónicos.

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 con lo mencionado, ya que no se realiza.

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.- Las personas encargadas, cuentan con algunas de las capacitaciones

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.

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

R.- Se ha ajustado todo lo correspondiente a datos personales conforme a lo establecido en la Ley General de Protección de Datos Personales en Posesión de Sujetos obligados.

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.- Nos ajustamos a lo señalado Ley General de Protección de Datos Personales en Posesión de Sujetos obligados, cada una de las áreas encargadas de la información generada, se enfocan con sumo cuidado a la protección de los datos personales, sin incurrir en violaciones a los mismos, por consiguiente no se cuenta con observación o sanción por parte del INAI.

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

R.- Si

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

R.- En caso de presentarse se aplica las políticas ya planteadas en el manejo, trata de información institucional y datos personales para comunicación.

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

R.- Las medidas son permanentes y solo se modifican en caso de ser necesario.

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

R.- No se realizan, se llevan a cabo mantenimientos periódicos y revisión de software y Hardware

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.

R.-Se cuenta con formato de solicitud de servicio, mediante el cual el servidor público especifica el problema presentado, en dichos formatos se describe la razón del problema al igual que su solución.

27. Informar sí se cuenta con un Centro de Operaciones de Ciberseguridad, Además informar si ha tenido incidentes de Ciberseguridad (sin Importar ni decir cuáles).

R.-. No se cuenta con el Centro de Operaciones de Ciberseguridad. No se han tenido incidentes relacionados con el mismo.

Sin más por el momento me despido enviándole un cordial saludo, quedo a sus órdenes para cualquier aclaración.

ATENTAMENTE

C.c.p. Archivo.