Asunto: **Resolución**
Número de Folio: **310573824000236**
Mérida, Yucatán, a 13 de noviembre de 2024

Para resolver la solicitud marcada con el folio **310573824000236** por lo que se procede a dictar la presente resolución con base en los siguientes:

ANTECEDENTES

PRIMERO. – Que con fecha 30 de octubre del año en curso a las 15:26 horas, el Departamento de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Estadística del Tribunal Superior de Justicia, recibió la solicitud de acceso a la información pública marcada con el folio **310573824000236**, misma que se tuvo como legalmente presentada al día siguiente hábil (31 de octubre de 2024), esto es por haberse recibido fuera del horario de labores.

SEGUNDO. - En la referida solicitud se requirió información en los siguientes términos*:*

"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;

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).

TERCERO. – Con base en lo anterior este Departamento, para dar el debido trámite, requirió la información instada mediante oficio número DTAIPE-TSJ-487/2024 al Departamento de Informática del Tribunal Superior de Justicia del Estado.

CUARTO. – Como resultado de lo señalado, se recopiló la información correspondiente; por lo que este Departamento, una vez agotado el procedimiento interno que tiene como finalidad estar en posibilidades de dar respuesta con la información requerida, para un mejor manejo se concentró la información en un documento anexo al presente, por lo que se emiten los siguientes:

CONSIDERANDOS

PRIMERO. - El Tribunal Superior de Justicia del Estado del Poder Judicial del Estado, es uno de los sujetos obligados por la Ley de Transparencia y Acceso a la Información Pública del Estado de Yucatán, conforme a lo establecido en el artículo 49, fracción III[1] de dicho ordenamiento.

SEGUNDO. - Que de acuerdo a lo establecido en el artículo 59 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Yucatán, la Unidad de Transparencia del Tribunal Superior de Justicia, es el vínculo entre los sujetos obligados y el solicitante, además tendrá la responsabilidad de recibir y dar trámite a las solicitudes de acceso a la información, del ámbito de su competencia.

TERCERO. - Que de conformidad con el artículo 63 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Yucatán, la información en posesión de los sujetos obligados es pública y únicamente estará sujeta al régimen de excepciones previsto en la Ley general y en dicha ley, por lo que del análisis de la información recopilada se determina que no se trata de información reservada o confidencial, en los términos de la ley de la materia, por lo que no existe excepción alguna para su publicidad.

Es por todo, lo antes expuesto, considerado y fundado, este Departamento de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Estadística del Tribunal Superior de Justicia del Estado:

RESUELVE

PRIMERO. - Póngase a disposición de la parte interesada sin costo a través de la Plataforma Nacional de Transparencia, un archivo electrónico que contiene la información recopilada al respecto.

---

[1] **Artículo 49.** Las disposiciones de la Ley general y esta ley se aplicarán, en calidad de sujetos obligados, a:
…
III. El Tribunal Superior de Justicia**,** el Consejo de la Judicatura y los tribunales que no sean administrados directamente por este, del Poder Judicial.
…"

SEGUNDO. - Infórmese a la parte interesada que la presente resolución puede ser impugnada a través del Recurso de Revisión en los plazos establecidos en las disposiciones legales aplicables.

TERCERO. - En caso de cualquier duda al respecto se orienta para que si es su voluntad se comunique al presente Departamento en los horarios de atención al público de lunes a viernes de 8:00 a 15:00 horas al teléfono 9999 30 06 50 Ext. 5024.

CUARTO. - Con fundamento en el artículo 125 de la Ley General de Transparencia y Acceso a la Información Pública, se realiza la presente notificación por la Plataforma Nacional de Transparencia, en virtud de ser el medio a través del cual se realizó la solicitud de información.

QUINTO. - Cúmplase.

Así lo resolvió y firma el jefe del Departamento de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Estadística, del Tribunal Superior de Justicia del Estado, Lic. Carlos Alberto Peraza Ávila, en la presente solicitud de información.

PODER JUDICIAL DEL ESTADO
YUCATÁN
TRIBUNAL SUPERIOR DE JUSTICIA
TRANSPARENCIA

Atentamente,

Lic. Carlos Alberto Peraza Ávila.
Jefe del Departamento