



**UNIDAD DE TRANSPARENCIA**

**EXPEDIENTE: 20/2024**

**ASUNTO: RESOLUCIÓN**

**NÚMERO DE FOLIOS: 310573724000031.**

**MÉRIDA, YUCATÁN, 06 DE NOVIEMBRE DE 2024.**

Para resolver la solicitud de acceso, presentada a través de la Plataforma Nacional de Transparencia, generando el número de folio **310573724000031**, se procede a dictar la presente resolución con base en los siguientes:

**ANTECEDENTES**

- I. Con fecha veintidós de noviembre del año 2024 el requirente presentó su solicitud de acceso a través de la Plataforma Nacional de Transparencia, generando el folio número **310573724000031**.
- II. En la referida solicitud el particular requirió información en los términos establecido en dicha solicitud.
- III. Con fecha veinticinco de octubre del año dos mil veinticuatro la Unidad de Transparencia requirió al área de Informática del Tribunal de los Trabajadores al Servicio del Estado y de los Municipios, al Ingeniero en Sistemas Luis Armando Echeverría Pérez por medio de oficio **TTSEM/UT32/2024** para que colabore e informe con respecto a la solicitud de acceso antes citada a fin de su debida substanciación.
- IV. El día cinco de noviembre del año dos mil veinticuatro el área de Informática turno oficio número **TTSEM/INF-0018/2024** a la Unidad de Transparencia, informando y adjuntando un anexo de 4 fojas tamaño carta, con las respuestas a las preguntas de la solicitud de acceso.

**CONSIDERANDO**

**PRIMERO.** - Que la unidad de Transparencia del Tribunal de los Trabajadores al Servicio del Estado y de los Municipios, tiene entre sus funciones recibir y dar trámite a las solicitudes de acceso a la información, según lo dispuesto en el artículo 45 fracciones II y IV de la Ley General de Transparencia y Acceso a la Información Pública, en correlación con los artículos 79, 80 y 81 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Yucatán.

Con base a lo anteriormente expuesto y fundado, la Unidad de Transparencia del Tribunal de los Trabajadores al Servicio del Estado y de los Municipios:

**RESUELVE**

**PRIMERO.** - Poner a disposición de quien solicita la presente resolución a través de la Plataforma Nacional de Transparencia, de conformidad con el considerando primero de la presente resolución.

**SEGUNDA.** - Infórmele al solicitante que la presente resolución puede ser impugnada a través del Recurso de Revisión en los plazos establecidos en la Ley General de Transparencia y Acceso a la Información Pública y en las demás disposiciones legales aplicables.

“2024, Año de Felipe Carrillo Puerto, Benemérito del Proletariado, Revolucionario y Defensor del Mayab”

**TERCERO.** - Notifíquese por medio de la Plataforma Nacional de Transparencia al solicitante de esta resolución.

Así lo resolvió y firma la responsable de la Unidad de Transparencia del Tribunal de los Trabajadores al Servicio del Estado y de los Municipios, Licenciada en Derecho Ady Marbella Vernon Caamal, en la ciudad de Mérida, Yucatán, a seis de noviembre del año 2024.

**ATENTAMENTE**



**Lic. Ady Marbella Vernon Caamal**  
**Responsable de la Unidad de Transparencia**  
**Del Tribunal de los trabajadores al Servicio del Estado**  
**Y de los Municipios.**



TRABAJADORES  
AL SERVICIO DEL ESTADO Y DE  
LOS MUNICIPIOS



TRIBUNAL DE LOS TRABAJADORES  
AL SERVICIO DEL ESTADO Y DE  
LOS MUNICIPIOS

**OFICIO NÚMERO: TTSEM/INF-0018/2024**

**ASUNTO: Respuesta a oficio TTSEM/UT32/2024**

Mérida, Yucatán, a 5 de noviembre de 2024.

**LIC. ADY MARBELLA VERMON CAAMAL.**  
**RESPONSABLE DE LA UNIDAD DE TRANSPARENCIA DEL**  
**TRIBUNAL DE LOS TRABAJADORES AL SERVICIO DEL ESTADO**  
**Y DE LOS MUNICIPIOS.**  
**PRESENTE**

Por medio de la presente, y en atención a su oficio número **TTSEM/UT32/2024** de fecha 25 de octubre de 2019, mediante el cual requirió la información correspondiente a la solicitud de acceso a la información pública registrada con el número de folio **310573724000031**, al respecto, y a fin de dar debido cumplimiento a dicha solicitud me permito enviarle la información requerida mediante un anexo escrito constante de 5 hojas útiles, mismo que se adjunta al presente oficio.

Sin otro particular por el momento, en espera de haber satisfecho los requerimientos del caso, le mando un cordial saludo.

Recibi  
Unidad de Transparencia  
05/nov/2024

**ATENTAMENTE**

**I.S.C. LUIS ARMANDO ECHEVERRIA PÉREZ**  
**ENCARGADO DEL DEPARTAMENTO DE INFORMÁTICA DEL TRIBUNAL DE LOS**  
**TRABAJADORES AL SERVICIO DEL ESTADO Y DE LOS MUNICIPIOS**



# ANEXO

1	informar si dentro de la institucion se cuenta con un gobierno de seguridad de la informacion o ciberseguridad y cuales areas participan	En respuesta a su solicitud, me permito informar que, no contamos con un gobierno formal de seguridad de la informacion o ciberseguridad. Esta situacion representa un area de oportunidad significativa para el fortalecimiento de nuestras capacidades defensivas en el ambito digital.
2	<p>Señalar si se cuenta con lo siguiente:</p> <p>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.</p> <p>b) informar si se cuenta con un inventario institucional de bienes y servicios de TIC.</p> <p>c) un plan de continuidad de operaciones, y señalar la fecha de implementación.</p> <p>d) informar si se ha desarrollado e implementado el plan de recuperación de desastres, señalar la fecha de desarrollo e implementación.</p> <p>e) desarrollado e implementado un programa de gestión de vulnerabilidades.</p> <p>f) marco de gestión de seguridad de la información (MGSI) o sistema de gestión de seguridad de la información (SGSI).</p> <p>g) informar si se cuenta con una política general de seguridad de la información y en su caso, quienes intervienen y desde cuando se implementó.</p> <p>h) 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.</p>	<p>En respuesta a su solicitud me permito informar por puntos:</p> <p>a) contamos con manual de "Procedimiento de Compra en Materia de Informática."</p> <p>b) contamos con inventario institucional de bienes y servicios.</p> <p>c) contamos con manual de "Protocolo para Respaldo en los Sistemas de Información", se ha implementado desde el 2021.</p> <p>d) contamos con el manual "Plan de Recuperación de Desastres en Materia de Informática." se desarrolló y se empezó a implementar desde el 2021.</p> <p>e) no contamos con un programa de gestión de vulnerabilidades. Esta situación representa un área de oportunidad significativa para el fortalecimiento de nuestras capacidades defensivas en el ámbito digital.</p> <p>f) no contamos con un programa de gestión de la información o sistema de gestión de seguridad. Esta situación representa un área de oportunidad significativa para el fortalecimiento de nuestras capacidades defensivas en el ámbito digital.</p> <p>g) no contamos con una política general de seguridad de la información. Esta situación representa un área de oportunidad significativa para el fortalecimiento de nuestras capacidades defensivas en el ámbito digital.</p> <p>h) contamos con manual de "Plan de Recuperación de desastres", se ha implementado desde el 2021.</p>

3	<p>informar si es que se cuenta con una estrategia de ciberseguridad dentro de la institución, en caso de respuesta afirmativa, informar lo siguiente:</p> <p>(1) referir la fecha de creación.  (2) la fecha de implementación.  (3) si es que se ha actualizado o modificado y en cuántas ocasiones.  (4) cuáles áreas participaron en la creación de dicha estrategia</p>	no contamos con una estrategia de ciberseguridad dentro de la institución. Esta situación representa un área de oportunidad significativa para el fortalecimiento de nuestras capacidades defensivas en el ámbito digital.
4	informar si se emplea la firma electrónica avanzada en la institución	no contamos con el uso de firma electrónica avanzada en la institución. Esta situación representa un área de oportunidad significativa para el fortalecimiento de nuestras capacidades defensivas en el ámbito digital.
5	informar si se realizan simulacros sobre el plan de recuperación de desastres o en caso de incidentes cibernéticos	si se realizan simulacros sobre el plan de recuperación de desastres y se realizan 2 veces al año.
6	Señalar si se cuentan con lineamientos de programación y desarrollo de sistemas informáticos seguros	no contamos con lineamientos de programación y desarrollo de sistemas informáticos. Esta situación representa un área de oportunidad significativa para el fortalecimiento de nuestras capacidades defensivas en el ámbito digital.
7	informar si los servicios de centros de datos son propios, de otra institución gubernamental o de un tercero	los servicios del centro de datos si son propios de la institución
8	informar si para el trabajo remoto se cuentan con lineamientos de seguridad para las videollamadas	no se realiza trabajo remoto
9	<p>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:</p> <p>a) inserción de leyenda de confidencialidad de la información o en su caso de transparencia y acceso a la Información</p> <p>c) control institucional de la totalidad de los correos contenidos en las carpetas de los usuarios</p> <p>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</p> <p>e) cuenta con cifrado en el envío de información.</p>	<p>si se cuenta con correo electrónico institucional, cuenta con leyenda de confidencialidad de la información.</p> <p>a) si cuenta con leyenda de confidencialidad de la información.</p> <p>c) contamos con un control institucional de la totalidad de correos.</p> <p>d) contamos con configuraciones de correo no deseado, así como programa que protege el envío y recepción de correos con software malicioso.</p> <p>e) contamos con cifrado en el envío de la información.</p>
10	informar si se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información institucional por parte de los servidores públicos.	no contamos con mecanismos para evitar la divulgación no autorizada de datos o información institucional. Esta situación representa un área de oportunidad significativa para el fortalecimiento de nuestras capacidades defensivas en el ámbito digital.



11	informar si la página web de la institución cuenta con: a) aviso de privacidad b) certificados digitales vigentes	nuestro sitio web institucional si cuenta con aviso de privacidad y 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	en lo que respecta a este protocolo, no se ha tomado esta capacitación
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 la madurez institucional en la gestión de seguridad de la información	no contamos con estos mecanismos. Esta situación representa un área de oportunidad significativa para el fortalecimiento de nuestras capacidades defensivas en el ámbito digital.
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	no contamos con un programa de formación en la cultura de la seguridad de la información. Esta situación representa un área de oportunidad significativa para el fortalecimiento de nuestras capacidades defensivas en el ámbito digital.
15	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.	no se cuenta con un sistema de gestión de protección de datos personales
16	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	nuestro modelo o sistema de comunicación para informar a la sociedad en general sobre eventos o incidentes de seguridad de la institución es mediante nuestro sitio web institucional
17	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	se informa de manera personal a cada usuario de los datos personales, esto es a través de correo electrónico u otro medio proporcionado por el particular
18	informar si se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos	no contamos con lineamientos para el traslado de activos físicos. Esta situación representa un área de oportunidad significativa para el fortalecimiento de nuestras capacidades defensivas en el ámbito digital.

19	informar si las personas encargadas de sistemas de información, donde se brinde información pública, cuentan con conocimientos comprobables en las siguientes materias: (1) transparencia (2) protección de datos personales (3) archivos públicos (4) seguridad de la información.	La única persona de brindar información es la encargada de la Unidad de Transparencia que se encuentra capacitada en todos estos conceptos
20	informar si han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas	no se han tenido brechas de ciberseguridad desde el año 2015 a la fecha.
21	informar si se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son	se implementa una configuración en un procesador de texto para apoyo en las versiones públicas en el ámbito de el manejo de información y datos personales
22	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	no contamos con plataforma informático u algun sistema en particular en virtud de falta de presupuesto del sujeto obligado.
23	Informar si se cuenta con documento de seguridad en materia de protección de datos personales;	contamos con el aviso de privacidad simplificado
24	informar si se cuenta con un plan de comunicación institucional en caso de un incidente de ciberseguridad o seguridad de la información.	se maneja con oficios internos
25	informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución.	cada que se requiera
26	informar si se llevan auditorias de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad	no se llevan acabo auditorias.
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	no se cuenta con un help desk
28	Señalar si las páginas web de los buscadores de versiones públicas de sentencias del Tribunal, tienen certificados digitales vigentes	si cuentan con certificados vigentes
29	informar si dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan	En respuesta a su solicitud, me permito informar que, no contamos con un gobierno formal de seguridad de la información o ciberseguridad. Esta situación representa un área de oportunidad significativa para el fortalecimiento de nuestras capacidades defensivas en el ámbito digital.
30	informar si es que se cuenta con una estrategia de ciberseguridad dentro de la institución, en caso de respuesta afirmativa, informar lo siguiente:  (1) referir la fecha de creación. (2) la fecha de implementación. (3) si es que se ha actualizado o modificado y en cuántas ocasiones. (4) cuáles áreas participaron en la creación de dicha estrategia	no contamos con una estrategia de ciberseguridad dentro de la institución. Esta situación representa un área de oportunidad significativa para el fortalecimiento de nuestras capacidades defensivas en el ámbito digital.



31	informar si se cuenta con un sistema de gestión de seguridad de la información dentro de la institución	no contamos con un sistema de gestión de seguridad de la información. Esta situación representa un área de oportunidad significativa para el fortalecimiento de nuestras capacidades defensivas en el ámbito digital.
32	informar si' 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	no se cuenta con un sistema de gestión de protección de datos personales
33	informar si es que se cuenta con un plan de continuidad del negocio, para el caso de algún evento o incidente de seguridad cibernética o física	contamos con el manual "Plan de Recuperación de Desastres en Materia de Informática." se desarrolló y se empezó a implementar desde el 2021.