Respuesta a solicitud de acceso a la información pública del estado de Yucatán

A quien corresponda:

En respuesta a la solicitud de acceso a la información pública del estado de Yucatán marcada con el número de folio 310573624000048, presentada el 30 de octubre de 2024, a las 15:126:18 P.M., por Qt(Sic), a través de la Plataforma Nacional de Transparencia, mediante la cual se solicita:

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 de conformidad con el Acuerdo por el que se emiten politicas y disposiciones para impulsar el uso y aprovechamiento de la informatica, el gobierno digital, las tecnologias de la información y la comunicación, y la seguridad de 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 pr la Coordinación de Estrategia Digital Nacional, en la contrataci,on de bienes y servicios de seguridad de la información o de lsa tecnológias de la información.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 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 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.*
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 seguridad 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.*
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 cuales)

Respuesta

Al respecto, resulta aplicable, de igual forma, el criterio de interpretación 03/17 emitido por el Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales:

> Criterio 03/17
>
> No existe obligación de elaborar documentos ad hoc para atender las solicitudes de acceso a la información. Los artículos 129 de la Ley General de Transparencia y Acceso a la Información Pública y 130, párrafo cuarto, de la Ley Federal de Transparencia y Acceso a la Información Pública, señalan que los sujetos obligados deberán otorgar acceso a los documentos que se encuentren en sus archivos o que estén obligados a documentar, de acuerdo con sus facultades, competencias o funciones, conforme a las características físicas de la información o del lugar donde se encuentre. Por lo anterior, los sujetos obligados deben garantizar el derecho de acceso a la información del particular, proporcionando la información con la que cuentan en el formato en que la misma obre en sus archivos; sin necesidad de elaborar documentos ad hoc para atender las solicitudes de información.
>
> Resoluciones:
>
> • RRA 0050/16. Instituto Nacional para la Evaluación de la Educación. 13 julio de 2016. Por unanimidad. Comisionado Ponente: Francisco Javier Acuña Llamas.

- RRA 0310/16. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. 10 de agosto de 2016. Por unanimidad. Comisionada Ponente. Areli Cano Guadiana.

- RRA 1889/16. Secretaría de hacienda y Crédito Público. 05 de octubre de 2016. Por unanimidad. Comisionada Ponente Ximena Puente de la Mora.

Atendiendo al principio de máxima publicidad, previsto por el artículo 6, Apartado A, fracción I de la Constitución Política de los Estados Unidos Mexicanos, nos permitimos informarle puntualmente lo siguiente:

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

Respuesta. Se informa que la Dirección de administración del Tribunal de Justicia Administrativa del Estado de Yucatán, tiene dentro de su estructura el área de informática.

"2. Señalar sí de conformidad con el Acuerdo por el que se emiten politicas y disposiciones para impulsar el uso y aprovechamiento de la informatica, el gobierno digital, las tecnologias de la información y la comunicación, y la seguridad de 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 contrataci,on de bienes y servicios de seguridad de la información o de lsa tecnológias de la información.se cuenta con lo siguiente: b) 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;

Respuesta: Se informa que de manera específica no se cuenta con 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"

Respuesta: La Dirección Administración informa que sí cuenta con un inventario institucional general de bienes muebles.

En ese sentido y en observancia al principio de Máxima Publicidad, es menester manifestar que, en caso de su interés, dicho inventario se encuentra disponible en la Plataforma Nacional de Transparencia, en el Sistema de Portales de Obligaciones de Transparencia (SIPOT), ya que se constituye como una obligación de transparencia común de los sujetos obligados, prevista en el artículo 70, fracción XXXIV (Inventario de bienes muebles) de la Ley General de Transparencia y Acceso a la Información Pública.

“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

Respuesta: El Tribunal no cuenta con un plan de operaciones, así como, un plan de recuperación ante desastres.

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

Respuesta: Actualmente, no se cuenta con un programa de gestión de vulnerabilidades, sin embargo, se realizan pruebas de vulnerabilidades para aquellas aplicaciones que son expuestas a internet o a solicitud del área de desarrollo.

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

Respuesta: El Área de Informática de la Dirección de Administración,Informática, en la actualidad no se trabaja bajo un conjunto de políticas de administración de la información como 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 implemen

Respuesta: Se informa que, no se cuenta con los lineamientos estipulados dentro de las “Políticas Generales en Materia de Tecnologías de la Información del Tribunal de Justicia Administrativa del Estado de Yucatán”

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

Respuesta: No se cuenta con un diagnóstico de identificación de sistemas de procesos.

“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”

Respuesta: Se informa que el Área de Informática de la Dirección de Administración, no cuenta con un servicio de 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”

Respuesta: Se informa que el Área de Informática de la Dirección de Administración, no ha elaborado estrategias de ciberseguridad.

“4. Informar si se emplea la firma electrónica avanzada en la institución”

Respuesta: Se informa que este Tribunal no emplea la Firma Electrónica Certificada.

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

Respuesta: Se informa que, no se llevan a cabo pruebas de replicación y restauración para diversos sistemas sustantivos del Tribunal.

“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: Se informa que, no se cuenta la contratación de servicios de seguridad de la información en Tecnologías de la Información y Comunicación y Seguridad de la Información.

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

Respuesta: Se informa que el Tribunal de Justicia administrativas del Estado de Yucatán, no se cuenta con centros de datos propios, ni de otra institución gubernamental.

“8. Informar sí se cuenta con un correo electrónico institucional; Si se cuenta con el correo institucional en la plataforma de Google Workspace 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; Si se cuenta con la leyenda, sin embargo, no está implementada en todos los correos de la institución. c) Control institucional de la totalidad de los correos contenidos en las carpetas de los usuarios”

Respuesta: Se cuenta con acceso a la consola de administración de correo electrónico proporcionada por la plataforma de thunderbird. No se cuenta con el correo institucional en la plataforma de Google Workspace 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; Se cuenta con el sistema de filtrado y los programas de protección propios de la plataforma de Google Workspace. 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”

Respueta: No se cuenta con esos mecanismos.

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

Respuesta: Los avisos de privacidad se encuentran disponibles en: https://tjay.org.mx/avisos-de-privacidad/; respecto del certificado se encuentra vigente

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

Respuesta: No, se cuenta con ésta 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; No se cuenta con esos mecanismos. b) Indicadores que permitan medir el madurez institucional en la gestión de seguridad de la información”

Respuesta: No se cuenta con esos indicadores.

“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”

Respuesta: No se cuenta con ese programa.

“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?”

Respuesta: No se cuenta con un sistema de gestión de protección de datos personales,

“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) ”

Respuesta: No se cuenta con el modelo de comunicación señalado.

“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 artículos 40, 41 y 42 de la Ley general de protección de datos personales en posesión de sujetos obligados (LGPDPPSO);; ”

Respuesta: No se cuenta con el modelo de comunicación señalado.

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

Respuesta: No se cuenta con los lineamientos señalados.

“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.”

Respuesta: Sí se cuenta con personal con conocimientos comprobables en las materias señaladas.

“19. Informar sí han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas”

Respuesta: No se han tenido brechas de seguridad en el periodo señalado.

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

Respuesta: No se han adoptado esquemas en materia de protección de datos personales.

“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”

Respuesta: No se cuenta con tal plataforma informática.

“22. Informar sí se cuenta con documento de seguridad en materia de protección de datos personales”

Respuesta: No se cuenta con el 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”

Respuesta: No se cuenta con el plan de comunicación señalado.

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

Respuesta: No se cuenta con las métricas señaladas.

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

Respuesta: No se han llevado auditorías en ciberseguridad.

“26. eñalar 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: No se cuenta con la herramienta señalada.

“2. Informar sí se cuenta con un Centro de Operaciones de Ciberseguridad. Además informar si han tenido incidentes de ciberseguridad(sin importar ni decir cuales)”

Respuesta: No se cuenta con Centro de Operaciones de Ciberseguridad

De igual forma, con fundamento en el artículo 142 de la Ley General de Transparencia y Acceso a la Información Pública, se hace de su conocimiento que, dentro de los quince días hábiles siguientes a la fecha de la notificación de la presente respuesta, podrá interponer recurso de revisión ante el Instituto Estatal de Transparencia, Acceso a la Información Pública y Protección de Datos Personales o ante esta Unidad de Transparencia.

Por otra parte, con fundamento en el artículo 125 de la Ley General de Transparencia y Acceso a la Información Pública, le informo que, con independencia de que la información pública sea proporcionada a través de la Plataforma Nacional de Transparencia, la respuesta a la solicitud de información constará, para su debida notificación, en los estrados de la Unidad de Transparencia del Tribunal de Justicia Administrativa del Estado de Yucatán.

Finalmente, agradecemos el interés mostrado al contactar al Tribunal de Justicia Administrativa del Estado de Yucatán. Es un honor para quienes integramos este Organismo Constitucional Autónomo poder atenderle y seguir avanzando en el fortalecimiento de la cultura de transparencia, así como en la promoción, respeto, protección y garantía de los derechos de acceso a la información pública y de protección de datos personales.

Nos reiteramos al servicio de la ciudadanía, estamos a sus órdenes.

Atentamente

(RÚBRICA)
Ing. Gabriel Ismael Sosa Valencia
Titular de la Unidad de Transparencia
del Tribunal de Justicia Administrativa del Estado de Yucatán

“Esta hoja de firma forma parte de la página 9 de 9 de la respuesta a la solicitud de acceso a la información pública del estado de Yucatán marcada con el número de folio 3105736240000048, presentada el 30 de octubre de 2024, a las 15:26:18 P.M.”