Dirección: Unidad de Transparencia,
Acceso a la Información Pública y
Protección de Datos Personales
Oficio: MT/UTAIPPDPT/0220/2024
Asunto: El que se indica

Tulum, Q. Roo, 08 de Noviembre de 2024.

ESTIMADO SOLICITANTE
P R E S E N T E:

En respuesta a su solicitud con número de folio **231288000025924,** realizado a través del **Plataforma Nacional de Transparencia (PNT**), de fecha de presentación e inicio de trámite 31 de Octubre de 2024, en la requiere la siguiente información:

"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 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 autoridad correspondiente;
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.

Tulum, Q. Roo, 08 de Noviembre de 2024.

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 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 artículos 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 artículos 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;

Dirección: Unidad de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
Oficio: MT/UTAIPPDPT/0220/2024
Asunto: El que se indica

Tulum, Q. Roo, 08 de Noviembre de 2024.

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).

Por lo anterior, en apego al principio de máxima transparencia establecido en lo previsto en los artículos 4, 11, 12, 13 párrafo primero, 45 fracciones II y V, y 123 y 129 de la Ley General de Transparencia y Acceso a la Información Pública; 3, 6, 11, 12, 13 párrafo primero, 66 fracciones II y V, 147, 148, 151 y 154 de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Quintana Roo. Asimismo, hago de su conocimiento que, los sujetos obligados en este asunto son:

UNIDAD ADMINISTRATIVA	No. DE OFICIO
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN.	OM/DTI/0140/2024

Y cuyo oficio se anexa a la presente solicitud de acceso a la información pública número de folio **231288000025924**, a continuación.

Se reitera el interés de esta Unidad de Transparencia en atender su solicitud, y se hace de su conocimiento, que aun, cuando la resolución contenida en el presente documento no vulnera su derecho de acceso a la Información pública, en caso de inconformidad por la misma, Usted tiene el derecho de Interponer su recurso de revisión ante el Instituto de Transparencia y Acceso a la Información Pública de Quintana Roo. Lo anterior de conformidad a lo establecido por el Titulo Noveno de la Ley en la materia.

Por lo anterior, se da por atendida en tiempo y forma su solicitud de información.
Sin otro particular, le envío un cordial saludo.

ATENTAMENTE

TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA TULUM, Q. ROO

LAET. LENNY JACQUELINE PÉREZ SALAZAR
"TITULAR DE LA UNIDAD DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES DE TULUM."

C.c.p. Archivo
RM

Dependencia: Oficialía Mayor.
Área: Dirección de Tecnologías de la Información.
Oficio: OM/DTI/0140/2024.
Asunto: Entrega de Información

Tulum, Q. Roo, 06 de Noviembre del 2024.

LAET. LENNY JACQUELINE PÉREZ SALAZAR
TITULAR DE LA UNIDAD DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES DEL H. AYUNTAMIENTO DE TULUM, Q.ROO.

PRESENTE:

Por medio del presente, me dirijo a usted de la manera más atenta y cordial, para darle seguimiento al **Oficio MT/UTAIPPDPT/0174/2024** de solicitud de información pública identificada con el número de folio de la plataforma Nacional de Transparencia (PNT) 231288000025924. conforme a lo establecido en los artículos 60,64,66 fracción IV, de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Quintana Roo, en relación a sus atribuciones conferidas en el Reglamento Interior del H. Ayuntamiento de Tulum, Quintana Roo.

De acuerdo a sus facultades establecidos en el Reglamento Interno de la Oficialía Mayor en los Artículos 40 del Reglamento Interior de la Oficialía Mayor de Tulum, Quintana Roo. de la Dirección de Tecnologías de la Información, por lo que le hago la entrega de dicha información solicita entregada de manera impresa y digital.

Sin otro particular me despido de usted quedando como su más atento y seguro servidor.

ATENTAMENTE.

DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN TULUM, QUINTANA ROO

MUNICIPIO DE TULUM
RECIBIDO
08 NOV. 2024 4:38 pm
UNIDAD DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES TULUM, QUINTANA ROO

ING. FRANCISCO ARANA SÁNCHEZ.
DIRECTOR DE TECNOLOGÍAS DE LA INFORMACIÓN DEL H. AYUNTAMIENTO DE TULUM.

C.c.p. Archivo
Elaboró Z.E M.Z
Revisó: JCCM
Autorizó FAS

Solicita la siguiente información:

1.- Informar si dentro de la institución se cuenta con un gobierno de seguridad de la información o de ciberseguridad y cuales áreas participan.

R: No se cuenta (Actualmente No se cuenta con ello, sin embargo, se planea implementar a la brevedad posible por la importancia que representa)

2.- Señalar si 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.

R: No se ha implementado (Actualmente no se cuenta con ello, sin embargo, se planea implementar a la brevedad posible por la importancia que representa).

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 servicio en materia de TIC y de seguridad de la información; informar si se cuenta con un inventario institucional de bienes y servicio de TIC

R: Si se cuenta

c) Un plan de continuidad de operaciones y señalar la fecha de implementación.

R: No se cuenta (Actualmente no se cuenta con ello, sin embargo, se planea implementar a la brevedad posible por la importancia que representa).

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

R: No se ha desarrollado e implementado (Actualmente no se cuenta con ello, sin embargo, se planea implementar a la brevedad posible por la importancia que representa).

e) Desarrollado e implementado un programa de gestión de vulnerabilidades.

R: No se ha desarrollado e implementado (Actualmente no se cuenta con ello, sin embargo, se planea implementar a la brevedad posible por la importancia que representa).

f) Marco de Gestión de Seguridad de la Información (MSGI).

R: No se ha implementado (Actualmente no se cuenta con ello, sin embargo, se planea implementar a la brevedad posible por la importancia que representa).

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.

R: No se cuenta (Actualmente no se cuenta con ello, sin embargo, se planea implementar a la brevedad posible por la importancia que representa).

h) Informar si se cuenta con un diagnóstico de identificación de los procesos y activos esenciales de la Institución.

R: No se cuenta (Actualmente no se cuenta con ello, sin embargo, se planea implementar a la brevedad posible por la importancia que representa).

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

R: No se cuenta (Actualmente no se cuenta con ello, sin embargo, se planea implementar a la brevedad posible por la importancia que representa).

3.- Informar si es que se cuenta con una estrategia de ciberseguridad dentro de la institución, en caso de respuesta afirmativa, informar lo siguiente:

R: No se cuenta

i) Referir la fecha de creación. **R: No aplica**
ii) La fecha de implementación. **R: No aplica**
iii) Si es que se ha actualizado o modificado y en cuantas ocasiones. **R: No aplica**
iv) Cuáles áreas participaron en la creación de dichas estrategias. **R: No aplica**

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

R: No se emplea

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

R: No se realizan

6.- Señalar si 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 autoridad correspondiente.

R: No se cuenta con Dictamen Técnico

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

R: Son propios y de otra institución gubernamental

8.- Informar si cuenta con un correo electrónico institucional e informa si el correo electrónico que se emplea en la institución cuenta con lo siguiente:

R: Si se cuenta con correo electrónico Institucional

a) Inserción de la leyenda de confidencialidad de la información. **R: Si**
b) Control Institucional de la totalidad de los correos contenidos en las carpetas e los usuarios. **R: Si**
c) 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. **R: Si**
d) Cuenta con cifrado en el envío de la información. **R: Si**

9.- Informar si se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información institucional por parte de los servidores públicos.

R: Si

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

a) Avisos de privacidad. **R: Si se cuenta**
b) Certificados digitales vigentes. **R: Si**

11.- Informar si el personal responsable, se ha capacitado en la Implementación del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos.

R: No (Actualmente no se ha recibido capacitación sin embargo se planea gestionarla a la brevedad posible por la importancia que representa).

12.- Informar si se cuenta con:

a) Los mecanismos de supervisión y evaluación que permitan medir la efectividad de los controles de seguridad de la información. **R: Si**
b) Indicadores que permitan medir la madurez institucional de la gestión de seguridad de la información. **R: No**

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 de afirmativo señalar. **R:** Cuando se implementó y cuantas horas de capacitación en ciberseguridad se realizan de forma anual.

R: No se cuenta

14.- Informar si de conformidad con la Ley General de Protección de Datos Personales 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 cuales áreas participaron en su desarrollo e implementación?

R: No se cuenta con un sistema de gestión de protección de datos personales (No han firmado algún documento de aviso de confidencialidad o 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 el caso de ser afirmativo, ¿Cuáles áreas de la Institución que participan? e informar desde cuando se implementó, lo anterior en términos de lo establecido por los artículos 40, 41 y 42 de la Ley general de protección de datos personales en posesión de sujetos obligados (LGPDPPSO).

R: No se cuenta

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 cuales áreas de la organización participan en su implementación y desde cuando se implementó, o anterior en términos de lo establecido por los artículos 40, 41 y 42 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO).

R: No se cuenta

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

R: No se cuenta

18.- Informar si las personas encargadas del sistema de información, donde se brinde Información pública, cuentan con conocimientos comprobables en las siguientes materias:

i)	Transparencia.	**R: Se desconoce**
ii)	Protección de datos personales.	**R: Se desconoce**
iii)	Archivos públicos.	**R: Se desconoce**
iv)	Seguridad de la información.	**R: Se desconoce**

La información solicitada no es competencia del área, por no brindar información pública conforma al artículo 40 del reglamento interior de Oficialía Mayor disponible en la siguiente liga https://tulum.gob.mx/

19.- Informar si han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuantas.

R: No existe registro anterior y a la fecha no se ha tenido brechas en esta administración.

20.- Informar si se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuales son.

R: No se cuenta (Actualmente no se cuenta con ello, sin embargo, se planea implementar a la brevedad posible por la importancia que representa).

21.- Informar si algún sistema o plataforma informática, aplicación electrónica o cualquiera 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 cuales han sido las recomendaciones vertidas por el del INAI, en su caso.

R: Existe un sistema que ha sido evaluado por parte de la autoridad competente, relacionada con el propio manejo del propio sistema administrativo SIGADI, mas no de la información contenida por no ser competencia de la Dirección de Tecnologías de la Información.

22.- Informar si se cuenta con documento de seguridad en materia de protección de datos personales.

R: No

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

R: No

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

R: No contamos con datos históricos

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

R: No

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.

R: Si

27.- Informa si se cuenta con un Centro de Operaciones de Ciberseguridad, además de informa si han tenido incidentes de ciberseguridad (sin importa ni decir cuales) (SIC).

R: No