Expediente número: **IEPCT-UTAIP/282/2024**
Solicitud folio: **270511500027624**

UNIDAD DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA DEL INSTITUTO ELECTORAL Y DE PARTICIPACIÓN CIUDADANA DE TABASCO VILLAHERMOSA, TABASCO, A TRECE DE NOVIEMBRE DE DOS MIL VEINTICUATRO. ---

Visto, De conformidad con lo establecido en los artículos 1, 7, 9, 10, 12 de la Ley General de Transparencia y Acceso a la Información Pública, 8, 24, 50 fracciones III y XI, 129 y 131 de la Ley de Transparencia y Acceso a la Información Pública vigente en el Estado de Tabasco.

Se acuerda- -

PRIMERO. El (21) de octubre del presente año, a las 15:57 horas**,** quien dice llamarse **XX** presentó solicitud electrónica registrada en el sistema Plataforma Nacional de Transparencia con el folio **270511500027624**, en la que requirió bajo el siguiente tenor:

"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 si 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 si 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 si se cuenta con un diagnóstico de identificación de los procesos y activos esenciales de la Institución; i) 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.**
3. **Informar si 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 si los servicios de centros de datos son propios, de otra institución gubernamental o de un tercero;**
8. **Informar si para el trabajo remoto se cuentan con lineamientos de seguridad para las video llamadas;**
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 si se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información Institucional por parte de los servidores públicos;**
11. **Informar si la página web de la institución cuenta con: a) aviso de privacidad; b) 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;**
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;**
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.**
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?;**
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;**
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;**
18. **Informar si se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos;**
19. **Informar si 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 si han tenido brechas de ciberseguridad desde el ario 2015 a la fecha de la presente solicitud y señalar cuántas;**
21. **Informar si se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son;**
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;**
23. **Informas si se cuenta con documento de seguridad en materia de protección de datos personales;**
24. **Informar si 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 si se llevan auditorias 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 si las páginas web de los buscadores de versiones públicas de sentencias del Tribunal, tienen certificados digitales vigentes.**

APARTADO2
Solicito la siguiente información.

29. **Informar si dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan;**
30. **Informar si 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) si es que se ha actualizado o modificado y en cuántas ocasiones; (iv) cuáles áreas participaron en la creación de dicha estrategia;**
31. **Informar si se cuenta con un sistema de gestión de seguridad de la información dentro de la institución;**
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?;**
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."**

SEGUNDO. Con fundamento en el artículo 137 de la ley de Transparencia y Acceso a la Información Publica del Estado de Tabasco que a la letra dice: *"las Unidades de Transparencia deberán garantizar que las solicitudes* ***se turnen a todas las áreas competentes*** *que cuenten con la información o* ***deban tenerla de acuerdo a sus facultades, competencias y funciones***". Esta Unidad de Transparencia turnó a la Secretaria Ejecutiva de este Instituto, toda vez que se trata de las áreas que le corresponde pronunciarse respecto de la información pretendida por el solicitante.

TERCERO. El (30) de octubre del año en curso, se tuvo por recibido ante esta Unidad de Transparencia el oficio **ESET/107/2024** suscrito por el Lic. José Juan Palma Silva, Enlace de la Secretaria Ejecutiva de este Instituto, es el área competente en este asunto. Para tal efecto se otorga la siguiente respuesta:

> "(…) Por lo anterior, adjunto al presente copia simple del oficio No. SE/UNITIC/664/2024, de fecha 29 de octubre del año en curso, signado por el Mtro. Raúl Olán León, Titular de la Unidad de Tecnologías de la Información y Comunicación, mediante el cual se da respuesta a la solicitud referida."

CUARTO. Con sustento en lo previsto por el artículo 138 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco, **se acuerda entregar el presente acuerdo al solicitante a través de la Plataforma Nacional de Transparencia.**

Asimismo, con fundamento en el artículo 129 de la Ley de Transparencia y Acceso a la Información Pública vigente en el Estado de Tabasco, se le comunica a la persona solicitante que en caso requerir cualquier orientación, quedamos a sus órdenes en las oficinas que ocupa esta Unidad de

Transparencia, sita en la calle Eusebio Castillo #747, colonia Centro, Código Postal 86000, así como en el teléfono 01 (993) 358 10 83, en horario de lunes a viernes de 09:00 a las 16:00 hrs.

Se hace saber a la persona solicitante que, de conformidad con el artículo 148 y 149 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco, en caso de no estar conforme con este acuerdo podrá interponer recurso de revisión, ante el Instituto Tabasqueño de Transparencia y Acceso a la Información Pública.

NOTIFÍQUESE el presente acuerdo a la persona solicitante, a través del Sistema Plataforma Nacional de Transparencia, con fundamento en lo dispuesto por los artículos 132, 133, y 138, primer párrafo, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco.

ASÍ LO ACORDÓ Y FIRMA LA TITULAR DE LA UNIDAD DE TRANSPARENCIA Y ACCESO ALA INFORMACIÓN PÚBLICA DEL INSTITUTO ELECTORAL Y DE PARTICIPACIÓN CIUDADANA DE TABASCO, LIC. JOSEFINA DIAZ DEL CASTILLO ROMERO.

INSTITUTO ELECTORAL Y DE PARTICIPACIÓN CIUDADANA DE TABASCO

Tu participación, es nuestro compromiso

SECRETARÍA EJECUTIVA

Oficio No. ESET/107/2024

Villahermosa, Tabasco; 30 de octubre de 2024

LIC. JOSEFINA DÍAZ DEL CASTILLO ROMERO
TITULAR DE LA UNIDAD DE TRANSPARENCIA
DEL IEPC TABASCO
P R E S E N T E.

En atención a su oficio **No. UTAIP/443/2024**, de fecha 25 de octubre del presente año, a través del cual remite la solicitud de acceso a la información pública con folio **270511500027624**, sin nombre del solicitante, mediante la cual se requiere información en archivo digital.

Por lo anterior, adjunto al presente copia simple del oficio No. SE/UNITIC/664/2024, de fecha 29 de octubre del año en curso, signado por el Mtro. Raúl Olán León, Titular de la Unidad de Tecnologías de la Información y Comunicación, mediante el cual se da respuesta a la solicitud referida.

Sin otro particular, le envío un cordial saludo.

A T E N T A M E N T E
"Tu participación, es nuestro compromiso."

INSTITUTO ELECTORAL Y DE PARTICIPACIÓN CIUDADANA DE TABASCO
IEPC TABASCO
SECRETARÍA EJECUTIVA
ENLACE ANTE LA UNIDAD DE TRANSPARENCIA

JOSÉ JUAN PALMA SILVA
ENLACE DE LA SECRETARÍA EJECUTIVA
ANTE LA UNIDAD DE TRANSPARENCIA

INSTITUTO ELECTORAL Y DE PARTICIPACIÓN CIUDADANA DE TABASCO
IEPC TABASCO
30 OCT 2024 12:52 hrs
RECIBIDO
Unidad de Transparencia
Recibí Original
Anexo 2 Fojas

C.c.p.- Lic. Jorge Alberto Zavala frías. – Secretario Ejecutivo del IEPCT. - Para su conocimiento.
C.c.p.-Archivo.

INSTITUTO ELECTORAL Y DE PARTICIPACIÓN CIUDADANA DE TABASCO

Unidad de Tecnologías de la Información y Comunicación UNITIC

SECRETARÍA EJECUTIVA
ENLACE ANTE LA UNIDAD DE TRANSPARENCIA
29.10.24
12:08 hrs.

Villahermosa, Centro, Tabasco, 29 de octubre de 2024
Oficio No. SE/UNITIC /664/2024

Asunto: Respuesta oficio ESET/103/2024

Lic. José Juan Palma Silva
Enlace de la Secretaría Ejecutiva
ante la Unidad de Transparencia
Presente

En atención a su oficio ESET/103/2024, solicitud de acceso a la información pública con folio 270511500027624, mediante el cual solicitan **respuesta al cuestionario enviado; a través del presente envío las respuestas de lo solicitado:**

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; **No**

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.
   a) **Se cuenta con un Inventario Institucional de bienes y servicios de Tic's. No se cuenta con ningún documento mencionado en los demás incisos.**

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 ; **No**
4. Informar sí se emplea la firma electrónica avanzada en la institución; **No**

5. Informar sí se realizan simulacros sobre el plan de recuperación de desastres o en caso de incidentes cibernéticos; **No**
6. Señalar si se cuentan con lineamientos de programación y desarrollo de sistemas informáticos seguros; **No**
7. Informar sí los servicios de centros de datos son propios, de otra institución gubernamental o de un tercero; **Propios**
8. Informar sí para el trabajo remoto se cuentan con lineamientos de seguridad para las videollamadas; **No**
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; **No**. c) control institucional de la totalidad de los correos contenidos en las carpetas de los usuarios; **Si.** 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; **No.** e) cuenta con cifrado en el envío de información. **No.**
10. Informar sí se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información Institucional por parte de los servidores públicos; **No**
11. Informar sí la página web de la institución cuenta con: a) aviso de privacidad; b) certificados digitales vigentes; **Si**
12. Informar sí el personal responsable se ha capacitado en la implementación del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos; **No**
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**
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. **No**
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?; **No**
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; **NO**
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; **No**

18. Informar sí se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos; **No**
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. **No**
20. Informar sí han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas; **No**
21. Informar sí se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son; **No**
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; **No**
23. Informas sí se cuenta con documento de seguridad en materia de protección de datos personales; **No**
24. Informar sí se cuenta con un plan de comunicación institucional en caso de un incidente de ciberseguridad o seguridad de la información; **No**
25. Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución; **En cada Proceso Electoral**
26. Informar sí se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad; **Solo cada Proceso Electoral**
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**
28. Señalar sí las páginas web de los buscadores de versiones públicas de sentencias del Tribunal, tienen certificados digitales vigentes. **Si**

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; **No**
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 ; **No**
31. Informar sí se cuenta con un sistema de gestión de seguridad de la información dentro de la institución; **No**
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?; **No**

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 e informar desde cuándo se implementó; **No**

Sin más por el momento aprovecho la ocasión para enviarle un saludo cordial.

UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN UNITIC

Atentamente

Mtro. Raúl Olán León
Titular de la Unidad de Tecnologías
de la Información y Comunicación

Con copias para:
- Mtra. Elizabeth Nava Gutiérrez. - Consejera Presidenta del IEPCT. - Para su conocimiento.
- Lic. Jorge Alberto Zavala Frías. - Secretario del IEPCT. - Para su conocimiento.
- Archivo Unidad de Tecnologías de la Información y Comunicación. -

Elaboró:
Diana Cristhel Ávalos Sánchez