



TRIBUNAL ELECTORAL DE TABASCO

UNIDAD DE ENLACE, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES.



Folio de Solicitud: 270511800011024.

Expediente: TET-SAIP-110/2024.

Cuenta: Con oficios números TET/SYST-19/2024, TET/SA/512/2024, y TET-UEAIP-229/2024, signados por el Encargado de la Unidad de Informática y Soporte Técnico, la Secretaría Administrativa, y el Jefe de la Unidad de Enlace y Acceso a la Información Pública del Tribunal Electoral de Tabasco, respectivamente. Conste.

ACUERDO DE DISPONIBILIDAD

Unidad de Enlace, Acceso a la Información Pública del Tribunal Electoral de Tabasco. Villahermosa, Tabasco, a trece de noviembre de dos mil veinticuatro.

Visto el oficio de cuenta, así como las documentales que obran en el expediente TET-SAIP-110/2024, de conformidad con lo previsto en los artículos 4 y 138 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco en vigor, relacionado con el diverso 36 de su Reglamento, se acuerda:

Primero. Solicitud de información. El pasado veintiuno de octubre de dos mil veinticuatro, se presentó solicitud de información mediante el Sistema Electrónico de Uso Remoto denominado SISA 2.0 -Tabasco, a la cual le fue asignado el número de folio **270511800011024.**

Dicha solicitud fue formulada en los siguientes términos:

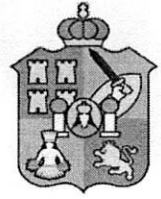
...”**APARTADO 1**

1. Informar si dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan;
2. Señalar si 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 si 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.



TRIBUNAL ELECTORAL DE TABASCO

UNIDAD DE ENLACE, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES.



Folio de Solicitud: 270511800011024.

Expediente: TET-SAIP-110/2024.

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) si es que se ha actualizado o modificado y en cuántas ocasiones; (iv) cuáles áreas participaron en la creación de dicha estrategia ;
4. Informar si se emplea la firma electrónica avanzada en la institución;
5. Informar si 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 videollamadas;
9. 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: 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 el 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.



TRIBUNAL ELECTORAL DE TABASCO

UNIDAD DE ENLACE, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES.



Folio de Solicitud: 270511800011024.

Expediente: TET-Saip-110/2024.

20. Informar si han tenido brechas de ciberseguridad desde el año 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. Informar 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 auditorías 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.

APARTADO 2

Solicito la siguiente información.

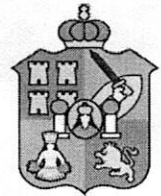
29. Informar si dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan;
30. Informar si es que se cuenta con una estrategia de ciberseguridad dentro de la institución, en caso de respuesta afirmativa, informar lo siguiente (i) referir 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" ... [sic]

Segundo. Competencia. Con fundamento en los artículos 6 y 8 de la Constitución Política de los Estados Unidos Mexicanos; 4 bis, fracción IV de la Constitución Política del Estado Libre y Soberano de Tabasco; 49 y 50 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco, la Unidad de Enlace, Acceso a la Información Pública y Protección de Datos Personales del Tribunal Electoral de Tabasco, es competente para tramitar y resolver la solicitud informativa de mérito.



TRIBUNAL ELECTORAL DE TABASCO

UNIDAD DE ENLACE, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES.



Folio de Solicitud: 270511800011024.

Expediente: TET-SAIP-110/2024.

Tercero. Integración de expediente. Mediante acuerdo datado el veintiuno de octubre del presente año, se analizaron los requisitos de procedibilidad de la presente solicitud de acceso a la información, integrándose el expediente interno con la clave alfanumérica TET-SAIP-110/2024, de conformidad con lo establecido en el artículo 50, fracciones III y V, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco, relacionada con el numeral 35 de su Reglamento.

Cuarto. Requerimiento a las áreas. En consecuencia, mediante oficios TET-UEAIP-210/2024, y TET-UEAIP-211/2024 se requirió a la Unidad de Informática y Soporte Técnico, así como a la Secretaría Administrativa, respectivamente, para que remitieran las informaciones solicitadas, acorde a sus atribuciones legales.

Quinto. Respuestas de las áreas. Se tienen por recibidos los oficio TET/SYST-19/2024, TET/SA/512/2024, y TET-UEAIP-229/2024, signados por el Encargado de la Unidad de Informática y Soporte Técnico, la Secretaría Administrativa, y el Jefe de la Unidad de Enlace y Acceso a la Información Pública del Tribunal Electoral de Tabasco, remitiendo la información solicitada, documental que se adjunta al presente acuerdo en formato PDF, para mayor constancia.

Sexto. Respuesta al solicitante. Con fundamento en los artículos 50, fracción VI, 138 y 139 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco, considerando la disponibilidad de la información solicitada, remítase la respuesta al peticionante de manera electrónica a través del sistema de solicitudes de acceso a la información de la PNT, de igual forma se encuentra localizada en la página del tribunal electoral de Tabasco, en la pestaña de transparencia, apartado de estrados electrónicos: http://www.tet.gob.mx/datasystem/Transparencia/Estrados/Estrados_Transparencia.php, carpeta del año 2024, bajo el rubro Acuerdo de Disponibilidad TET-SAIP-110-2024, con la finalidad de dar contestación en tiempo y forma a la solicitud realizada, bajo los principios de máxima publicidad y derecho de acceso a la información pública.

Séptimo. Notificación. Toda vez que el peticionario presentó su solicitud de acceso a la información por la vía electrónica antes mencionada, notifíquese el presente acuerdo por el mismo medio, conforme a lo dispuesto por el artículo 50, fracción VI y 132 de la Ley de



TRIBUNAL ELECTORAL DE TABASCO

UNIDAD DE ENLACE, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES.



Folio de Solicitud: 270511800011024.



Expediente: TET-SAIP-110/2024.

Transparencia y Acceso a la Información Pública del Estado de Tabasco y 39 fracción II, de su Reglamento. Cúmplase.

Octavo. Archivo. Hecho lo anterior, archívese ordenadamente, como asunto total y legalmente concluido.

Noveno. Recurso de revisión. Hágase del conocimiento del solicitante, que en términos de los artículos 148, 149 y 150 la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco, así como de los diversos 51 y 52 de su Reglamento, puede interponer **recurso de revisión** ante el Instituto Tabasqueño de Transparencia y Acceso a la Información Pública, ubicado en la calle José Martí 102, fraccionamiento Lidia Esther, Villahermosa, Tabasco, teléfono (993)1433999, o en la dirección electrónica www.itaip.org.mx; o en su caso, ante esta Unidad de Transparencia; ello, dentro de los **quince días hábiles** siguientes a la notificación del presente acuerdo.

Así lo acuerda, manda y firma el **L.D. Felipe Gustavo Bulnes Zurita**, Jefe de la Unidad de Enlace y Acceso a la Información Pública del Tribunal Electoral de Tabasco.



UNIDAD DE ENLACE

ELECTORAL



VILLAHERMOSA, TAB., 4 DE NOVIEMBRE DEL 2024

ASUNTO Contestación al Oficio
TET/UEAIP/210/2024

OFICIO No: TET/SYST-19/2024

LD Felipe Gustavo Bulnes Zurita
Jefe de Unidad de Enlace a la Información Pública
y Protección de datos Personales
P R E S E N T E

Por medio del presente, describo lo solicitado en el oficio TET/UEAIP/210/2024 en el cual se realizan una serie de cuestiones las cuáles de contestan a continuación:

..."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 SE CUENTA.

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;

NO SE HA IMPLEMENTADO.

c) un plan de continuidad de operaciones, y señalar la fecha de implementación;

NO SE CUENTA.

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

NO SE HA DESARROLLADO.

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



NO SE HA DESARROLLADO.

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

NO SI TIENE UN MARCO DE GESTION.

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;

NO SE CUENTA CON NINGUNA POLITICA.

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

NO SE CUENTA CON NINGUN DIAGNOSTICO.

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.

NO SE CUENTA CON UN EQUIPO, SIN EMBARGO EXISTE UN ÁREA DE INFORMATICA LA CUAL APOYA CON DIVERSOS TEMAS.

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, (ii) sí es que se ha actualizado o modificado y en cuántas ocasiones; (iv) cuáles áreas participaron en la creación de dicha estrategia;

NO SE CUENTA.

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

NO SE REALIZAN.



6. Señalar si se cuentan con lineamientos de programación y desarrollo de sistemas informáticos seguros;

ACTUALMENTE LOS SISTEMAS QUE MANEJA EL TRIBUNAL SON LOCALES ES DECIR NO ESTAN PUBLICADOS EN LA WEB, POR LO ANTERIOR NO ESTAN EXPUESTOS A ATAQUES DE DDOS Y CUENTAN CON LAS MEDIDAS BASICAS DE DESARROLLO CONO NO INYECCION DE SQL, CIFRADOS Y ENCRIPTADOS ENTRE LOS PRICIPALES.

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

LOS SERVICIOS SON PROPIOS DE ESTE TRIBUNAL.

8. Informar sí para el trabajo remoto se cuentan con lineamientos de seguridad para las videollamadas;

NO SE CUENTA.

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.

SI SE CUENTA CON UN CORREOS INSTITUCIONALES QUE CUMPLE CON LOS PUNTOS MENCIONADOS.

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



NO SE HA CAPACITADO.

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;

NO SE CUENTAN.

b) Indicadores que permitan medir la madurez institucional en la gestión de seguridad de la información;

NO SE CUENTAN.

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 SE CUENTA.

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.

SE CUENTA CON LOS CONOCIMIENTOS BASICOS EN LAS MATERIA MENSIONADAS.

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 INSIDENTES EN CUANTO A SEGURIDAD A LA FECHA.

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 INAI, en su caso;
NO SE CUENTA.

24. Informar si se cuenta con un plan de comunicación institucional en caso de un incidente de ciberseguridad o seguridad de la información;
NO SE CUENTA.

25. Informar cada cuanto tiempo se actualizan las medidas de ciberseguridad dentro de la institución;
SE LLEVA ACABO ACTUALIZACIONES DE LOS FIREWALL DE LA INSTITUCIÓN.

26. Informar si se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad;
NO SE LLEVAN 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 HELP DESK SIN EMBARGO LAS NECESIDADES SON SOLVENTADAS POR EL AREA DE INFORMATICA.

28. Señalar si las páginas web de los buscadores de versiones públicas de sentencias del Tribunal, tienen certificados digitales vigentes.
ACTUAL MENTE ESTA EN PROCESO DE ADQUISICIÓN DE LOS CERTIFICADOS.

APARTADO 2

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;
NO SE CUENTA.



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 SE CUENTA.

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" [sic]
contenidos en las carpetas de los usuarios;
NO SE CUENTA

Sin más por el momento me despido enviándole un cordial saludo.

ATENTAMENTE

Soporte Técnico

Ing. Manuel de Jesús Vega Luna



"2024, Año de Felipe Carrillo Puerto, Benemérito del Proletariado, Revolucionario y Defensor del Mayab"
Villahermosa, Tabasco a 12 de noviembre de 2024

Oficio No. TET/SA/512/2024

Asunto: Contestación TET/UEAIP-211/2024

L. D. Felipe Gustavo Bulnes Zurita
Jefe de la Unidad de Enlace, Acceso a la Información Pública
Y Protección de Datos Personales
Presente.

En respuesta a su similar TET-UEAIP-211/2024, en donde se refiere a la solicitud de transparencia con número 2705118000011024:

"[...] **4.** Informar si se emplea la firma electrónica avanzada en la institución; **16.** Informar si se cuentan 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 participan? e informar desde cuando 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; **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; [...]"

En respuesta, adjunto la información requerida.

Pregunta	Respuesta
4. Informar si se emplea la firma electrónica avanzada en la institución.	Si, se emplea.
16. Informar si se cuentan 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 participan? e informar desde cuando se implementó	No.
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.
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	Se cuenta con un buzón interno (físico) para tales efectos.



Sin más que agregar, quedo atenta a sus comentarios.

ATENTAMENTE

Brenda del Carmen Olán Custodio
Secretaria Administrativa





TRIBUNAL ELECTORAL DE TABASCO
UNIDAD DE ENLACE, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES

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

OFICIO	TET-UEAIP-229/2024
EXPEDIENTE	TET-SAIP-110/2024
FECHA	Villahermosa, Tabasco a 12 de noviembre de 2024

Estimado solicitante
Presente

Con motivo de la solicitud de información con folio **270511800011024**, presentada el veintiuno de octubre, mediante Plataforma Nacional de Transparencia, mediante la cual solicita a este sujeto obligado, lo siguiente:

..."APARTADO 1

1. Informar si dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan;
2. Señalar si 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 si 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) si es que se ha actualizado o modificado y en cuántas ocasiones; (iv) cuáles áreas participaron en la creación de dicha estrategia ;
4. Informar si se emplea la firma electrónica avanzada en la institución;
5. Informar si 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 videollamadas;
9. 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: 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 el 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 año 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. Informar 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 se actualizan las medidas de ciberseguridad dentro de la institución;
26. Informar si se llevan auditorías 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.

APARTADO 2

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



TRIBUNAL ELECTORAL DE TABASCO

UNIDAD DE ENLACE, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES

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

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." (sic)

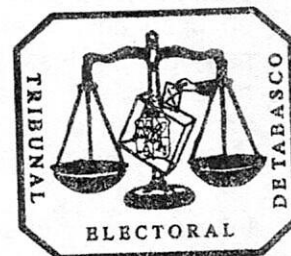
Al respecto me permito informarle, con base al ámbito de competencia de la Unidad Administrativa a mi cargo, lo siguiente:

Número	Pregunta	Respuesta
10	Informar si se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información Institucional por parte de los servidores públicos.	Sí, las establecidas en la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco, concernientes a aquella información que se establezca como información confidencial, o de carácter reservado.
11	Informar si la página web de la institución cuenta con: a) aviso de privacidad; b) certificados digitales vigentes.	a) Sí se cuenta.
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?	Este Sujeto Obligado cuenta con un Documento de Seguridad, en donde participaron las diversas Unidades Administrativas que resguardan información personal y/o de carácter confidencial, mismas que se encuentran detalladas en dicho documento. Consultable en la siguiente dirección electrónica: http://www.tet.gob.mx/datasystem/Transparencia/Documento%20de%20Seguridad.pdf
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.	Este Sujeto Obligado cuenta con un Documento de Seguridad, en donde participaron las diversas Unidades Administrativas que resguardan información personal y/o de carácter confidencial, mismas que se encuentran detalladas en dicho documento. Consultable en la siguiente dirección electrónica: http://www.tet.gob.mx/datasystem/Transparencia/Documento%20de%20Seguridad.pdf

		<u>nsparencia/Documento%20de%20Seguridad.pdf</u>
21	Informar sí se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son	Aún no se han adoptado nuevos esquemas, además de los ya vigentes.
23	Informar sí se cuenta con documento de seguridad en materia de protección de datos personales	Sí, consultable en la siguiente dirección electrónica: <u>http://www.tet.gob.mx/datasystem/Tra nsparencia/Documento%20de%20Seg uridad.pdf</u>
31	Informar sí se cuenta con un sistema de gestión de seguridad de la información dentro de la institución.	Sí, consultable en la siguiente dirección electrónica: <u>http://www.tet.gob.mx/datasystem/Tra nsparencia/Documento%20de%20Seg uridad.pdf</u>
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?	Este Sujeto Obligado cuenta con un Documento de Seguridad, en donde participaron las diversas Unidades Administrativas que resguardan información personal y/o de carácter confidencial, mismas que se encuentran detalladas en dicho documento. Consultable en la siguiente dirección electrónica: <u>http://www.tet.gob.mx/datasystem/Tra nsparencia/Documento%20de%20Seg uridad.pdf</u>

Sin otro particular por el momento, le saludo cordialmente.

ATENTAMENTE .

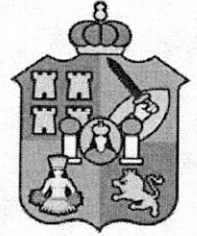
LD. Felipe Gustavo Bulnes Zurita **UNIDAD DE ENLACE**
Jefe de la Unidad de Enlace, Acceso a la Información Pública
y Protección de Datos Personales

c.c.p. Archivo.



TRIBUNAL ELECTORAL DE TABASCO

UNIDAD DE ENLACE, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES.



Folio de Solicitud: 270511800011024.

Expediente: TET-SAIP-110/2024

Vistos, para atender la solicitud de acceso a la información presentada a las **15:57** horas del veintiuno de octubre de dos mil veinticuatro, mediante el Sistema Electrónico denominado SISAI 2.0 de la Plataforma Nacional de Transparencia, a la que le fue asignada el número de folio **270511800011024**.

En consecuencia, con fundamento en lo previsto en los artículos 4, 49, 50 fracciones II, III, V y XI, 129, 131 y 137 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco, la suscrita **acuerda**:

ACUERDO DE INICIO

Unidad de Enlace, Acceso a la Información Pública y Protección de Datos Personales del Tribunal Electoral de Tabasco, Villahermosa, Tabasco, a veintiuno de octubre de dos mil veinticuatro.

Primero. Análisis de requisitos. De conformidad con lo dispuesto en el artículo 131 de la Ley de Transparencia y Acceso a la información Pública del Estado de Tabasco, se procede a analizar los requisitos de la solicitud de información que nos ocupa, con base en los datos siguientes:

- **Sujeto Obligado:** Tribunal Electoral de Tabasco.
- **Folio de la Solicitud:** 270511800011024

Información solicitada:

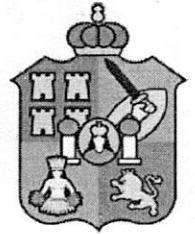
"APARTADO

1. Informar si dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan;
2. Señalar si 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



TRIBUNAL ELECTORAL DE TABASCO

UNIDAD DE ENLACE, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES.



Folio de Solicitud: 270511800011024.

Expediente: TET-SAIP-110/2024

Información (MGSI) o Sistema de Gestión de Seguridad de la Información (SGSI); g) Informar si 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) si es que se ha actualizado o modificado y en cuántas ocasiones; (iv) cuáles áreas participaron en la creación de dicha estrategia ;

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

5. Informar si 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 videollamadas;

9. 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: 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 el 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?;

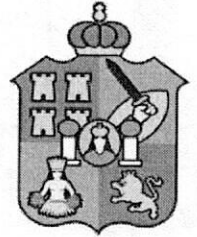
16. Informar si se cuenta con un modelo o sistema de comunicación, para informar a la sociedad en general sobre los eventos o incidentes de seguridad de la institución, y en caso de ser afirmativo, ¿cuáles áreas de la institución que participan? e informar desde cuándo se implementó;

17. Informar sobre si se cuenta con un modelo o sistema de comunicación para informar a los titulares



TRIBUNAL ELECTORAL DE TABASCO

UNIDAD DE ENLACE, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES.



Folio de Solicitud: 270511800011024.

Expediente: TET-SAIP-110/2024

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 año 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. Informar 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 se actualizan las medidas de ciberseguridad dentro de la institución;

26. Informar si se llevan auditorías 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.

APARTADO 2

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;

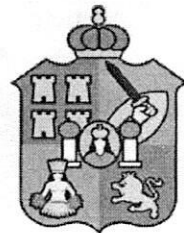
32. Informar si de conformidad con la Ley General de Protección de Datos Personales en Posesión de Particulares se cuenta con lo siguiente Un sistema de gestión de protección de datos personales, en caso de ser afirmativa esta pregunta, ¿desde cuándo se adoptó y cuáles áreas participaron en su desarrollo 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" [sic]



TRIBUNAL ELECTORAL DE TABASCO

UNIDAD DE ENLACE, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES.



Folio de Solicitud: 270511800011024.

Expediente: TET-SAIP-110/2024

Domicilio o forma en que desea ser notificado: Toda vez que el peticionario presentó su solicitud de acceso a la información por la vía electrónica denominada "Plataforma Nacional de Transparencia", téngase como domicilio para recibir notificaciones y/o la forma en como desea ser notificado, conforme a lo dispuesto por el artículo 50, fracciones III y VI y 132 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco, así como cualquier otro medio electrónico.

- **Modalidad por la cual desea recibir la información:** PNT

Segundo. Integración de expediente. De conformidad con el arábigo 50, fracción V, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco, intégrese el expediente respectivo con la clave alfanumérica **TET-SAIP-110/2024**, en el cual se glosarán los documentos y acuerdos recaídos a la presente solicitud de acceso a la información, para los efectos legales correspondientes.

Así lo acuerda, manda y firma el **L.D. Felipe Gustavo Bulnes Zurita**, Jefe de la Unidad de Enlace, Acceso a la Información Pública y Protección de Datos Personales del Tribunal Electoral de Tabasco.



UNIDAD DE ENLACE

ELECTORAL