Acuse de registro de solicitud de información pública

Se ha recibido exitosamente su solicitud de información pública, con los siguientes datos:

Datos de la Solicitud

Sujeto Obligado	TRIBUNAL SUPERIOR DE JUSTICIA (TSJ)
Folio	271473900029424
Fecha de solicitud	21/10/2024
Nombre del solicitante	
Representante (en su caso)	

Detalle de la Solicitud

Información requerida	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 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 si se cuentan con lineamientos de programación y desarrollo de sistemas informáticos seguros; 7. Informar sí los servicios de centros de datos son propios, de otra institución gubernamental o de un tercero; 8. Informar sí para el trabajo remoto se cuentan con lineamientos de seguridad para las videollamadas; 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 sí se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información Institucional por parte de los servidores públicos; 11. Informar sí la página web de la institución cuenta con: a) aviso de privacidad; b) certificados digitales vigentes; 12. Informar sí 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 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.
Datos adicionales	15. Informar sí de conformidad con la Ley General de Protección de Datos Personales en Posesión de

Acuse de registro de solicitud de información pública

Datos adicionales	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 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; 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; 18. Informar sí se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos; 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. 20. Informar sí han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas; 21. Informar sí se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son; 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; 23. Informas sí se cuenta con documento de seguridad en materia de protección de datos personales; 24. Informar sí 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 sí 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 sí 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 sí dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan; 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 ; 31. Informar sí se cuenta con un sistema de gestión de seguridad de la información dentro de la institución; 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?; 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
Medio de notificación	Electrónico a través del Sistema de Solicitudes de Acceso a la Información de la PNT

* Especificar de manera clara y precisa los datos e información que requiere.
* No incluir datos personales.

Plazos de respuesta

Respuesta a la Solicitud (Positivo, negativo o inexistencia)	15 días hábiles	13/11/2024
Requerimiento de información (Prevención)	5 días hábiles	29/10/2024
Incompetencia	3 días hábiles	25/10/2024

21/10/2024 15:57:42 PM

Acuse de registro de solicitud de información pública

La solicitud recibida en día hábil después de las 16:00 horas, o en día inhábil, se tendrá por presentada al siguiente día hábil según el calendario aprobado por el H. Pleno del Instituto Tabasqueño de Transparencia y Acceso a la Información Pública.
Los plazos señalados empezaran a correr al día siguiente de recibida la solicitud (LTAIPET).

RECOMENDACIONES:
*Dar seguimiento frecuente a la solicitud.

Tel. 99 35 92 27 80 ext. 4013 y 4082
Independencia esq. Nicolás Bravo s/n
Col. Centro, C. P. 86000, Villahermosa,

Folio PNT: 271473900029424
Número de Expediente Interno: PJ/UTAIP/289/2024
Acuerdo con Oficio No.: TSJ/UT/1136/2024
ACUERDO DE SOLICITUD NO PRESENTADA.

Villahermosa, Tabasco a 14 de noviembre de 2024.

VISTOS: Para atender la Solicitud de Acceso a la Información Pública, realizada el veintiuno de octubre de dos mil veinticuatro a las quince horas con cincuenta y siete minutos, y registrada bajo el número de expediente **PJ/UTAIP/289/2024**, en la que se solicita lo siguiente:

"...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 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.

Tel. 99 35 92 27 80 ext. 4013 y 4082
Independencia esq. Nicolás Bravo s/n
Col. Centro, C. P. 86000, Villahermosa,

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

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

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

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 sí se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información Institucional por parte de los servidores públicos;

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

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

Tel. 99 35 92 27 80 ext. 4013 y 4082
Independencia esq. Nicolás Bravo s/n
Col. Centro, C. P. 86000, Villahermosa,

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 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.

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?;

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;

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;

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

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.

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

Tel. 99 35 92 27 80 ext. 4013 y 4082
Independencia esq. Nicolás Bravo s/n
Col. Centro, C. P. 86000, Villahermosa,

21. Informar sí se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son;

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;

23. Informas sí se cuenta con documento de seguridad en materia de protección de datos personales;

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

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 ;

31. Informar sí se cuenta con un sistema de gestión de seguridad de la información dentro de la institución;

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?;

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;

34. 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;

35. 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;

36. Informar sí se realiza capacitación continua a los servidores públicos en materia de ciberseguridad y cada cuándo se lleva a cabo, así como los temas que se abordan;

37. Informar sí se cuenta con un procedimiento en caso de detección de alguna amenaza o vulneración de seguridad y cuál es el área encargada de atender los reportes;

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

39. Informar sí las personas encargadas de sistemas de información, donde se brinde información pública, cuentan con conocimientos comprobables en las siguientes

Tel. 99 35 92 27 80 ext. 4013 y 4082
Independencia esq. Nicolás Bravo s/n
Col. Centro, C. P. 86000, Villahermosa,

materias (i) transparencia; (ii) protección de datos personales; (iii) archivos públicos; o, (iv) seguridad de la información.

40. Informar sí han tenido brechas de ciberseguridad desde el año 2014 a la fecha de la presente solicitud y señalar cuántas;

41. Informar sí se cuenta con un modelo de madurez de seguridad de la información o ciberseguridad dentro de la institución, en caso afirmativo informar desde cuándo se implementa;

42. Informar sí se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son;

43. 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 ey 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;

44. Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución;

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

46. Señalar si se cuenta con un sistema de gestión de incidentes y cuáles áreas de la institución participan en este;

47. 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.

48. Señalar si se cuenta con un equipo de respuesta a incidentes cibernéticos, especificar si es interno o externo.

APARTADO 3

49.Indicar si cuenta con alguna solución tecnológica para juicios en línea, tribunal virtual, e-justice, justicia electrónica, ciberjusticia, ciberseguridad o inteligencia artificial.

50.En caso de contar con alguna solución para el propósito antes señalado, indicar el nombre de la solución tecnológica, dirección de internet donde es accesible, año de inicio de operaciones, materia legal del juicio de la materia de su competencia.

51.En caso de que no cuente con una solución tecnológica para este propósito y tiene conocimiento de alguno en su entidad, favor de indicar el sujeto obligado que pudiera contener dicha información. Me gustaría saber de qué manera aplican medios, instrumentos o aplicaciones que hagan uso de inteligencia artificial dentro del funcionamiento interno de su institución o al momento de brindar servicios a la ciudadanía. En caso de que no, saber si se tienen proyectos para aplicar dicho tipo de tecnología. A su vez se pide conocer lo siguiente:

52.Qué programas, algoritmos, sistemas de inteligencia artificial, sistemas de decisiones judiciales asistidas, algoritmos o programas de selección aleatoria de casos a jueces, tiene y opera.

53.El número de registros existentes de lo solicitado en el punto anterior.

a. Las fechas de operación.

b. El funcionamiento y operación de cada sistema o algoritmo con el que cuenta.

c. Los contratos de su uso o adquisición.

54. ¿Cómo procede y opera la selección y asignación aleatoria de casos a los jueces y juzgados en todas las materias? ¿Cómo se garantiza la independencia judicial a través de estos sistemas se selección y asignación aleatoria de casos?

55. ¿Qué datos se utilizan para la selección y asignación aleatoria de casos?...(sic)…"--

---

A C U E R D O

PRIMERO.- En virtud de la constancia que obra en los autos del expediente en que se actúa, se advierte que **HA FENECIDO**, el plazo de **DIEZ DÍAS HÁBILES**, concedido a el solicitante, para que formulara su petición en el sentido de **"la identificación clara y precisa de los datos e información que se requiere, señalando documento alguno en sus puntos de los cuales requiere la información"**, en la solicitud de acceso a la información recibida el veintiuno de octubre de dos mil veinticuatro y toda vez que se le solicitó que indicara, o aclarase que documento o documentos requería de este Sujeto Obligado, el peticionario no atendió debidamente el proveído que fue enviado vía Plataforma Nacional de Transparencia el veintinueve de octubre del dos mil veinticuatro, Ya que únicamente se limitó a repetir por segunda ocasión sus preguntas inquisitivas, sin indicar algún elemento nuevo o proporcionar mayor dato del documento que requería, es decir, no realizó aclaración alguna respecto de su solicitud original, razón por la que se considera la solicitud de acceso a la información, como no presentada para todos los efectos legales a que haya lugar. En consecuencia, se emite el presente acuerdo de conformidad con el artículo 131 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco.

NOTIFÍQUESE POR LA PLATAFORMA NACIONAL DE TRANSPARENCIA Y CÚMPLASE, ASÍ LO ACUERDA, MANDA Y FIRMA, LA DIRECTORA DE LA UNIDAD DE TRANSPARENCIA Y ACCESO A LA INFORMACION DEL PODER JUDICIAL, EN LA CIUDAD DE VILLAHERMOSA, CAPITAL DEL ESTADO DE TABASCO, A CATORCE DE NOVIEMBRE DE DOS MIL VEINTICUATRO. ----------CONSTE.----------

Esta hoja de firmas corresponde al Acuerdo de Solicitud No Presentada de fecha 14 de noviembre de 2024, dictado en el expediente relativo a la solicitud de información identificada con el número de folio 271473900029424. ----------

PODER JUDICIAL DEL ESTADO DE TABASCO