

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

<p>APARTADO 1</p> <p>1. Informar si dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan;</p> <p>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.</p> <p>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 ;</p> <p>4. Informar si se emplea la firma electrónica avanzada en la institución;</p> <p>5. Informar si se realizan simulacros sobre el plan de recuperación de desastres o en caso de incidentes cibernéticos;</p> <p>6. Señalar si se cuentan con lineamientos de programación y desarrollo de sistemas informáticos seguros;</p> <p>7. Informar si los servicios de centros de datos son propios, de otra institución gubernamental o de un tercero;</p> <p>8. Informar si para el trabajo remoto se cuentan con lineamientos de seguridad para las videollamadas;</p> <p>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.</p> <p>10. Informar si se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información Institucional por parte de los servidores públicos;</p> <p>11. Informar si la página web de la institución cuenta con: a) aviso de privacidad; b) certificados digitales vigentes;</p> <p>12. Informar si el personal responsable se ha capacitado en la implementación del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos;</p> <p>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;</p> <p>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.</p>	<p>Información requerida</p>
<p>15. Informar si de conformidad con la Ley General de Protección de Datos Personales en Posesión de</p>	<p>Datos adicionales</p>

Acuse de registro de solicitud de información pública

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. 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 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

Datos adicionales

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

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.



Folio PNT: 271473900029424
Número de Expediente Interno: PJ/UTAIP/289/2024
Acuerdo con Oficio No.: TSJ/UT/1072/2024
ACUERDO DE PREVENCIÓN.

Villahermosa, Tabasco a 29 de octubre de 2024.

CUENTA: Derivado de la solicitud de información efectuada mediante escrito con folio No. 271473900029424 enviada a través de la Plataforma Nacional de Transparencia, el veintiuno de octubre de dos mil veinticuatro a las quince horas con cincuenta y siete minutos; la cuál fue dirigida al Poder Judicial, y recibida por esta Unidad de Acceso, con fecha diecisiete de octubre de los corrientes; me permito informar a Usted, los siguientes: -----

HECHOS

PRIMERO: Con fecha del 21 de octubre de dos mil veinticuatro a las quince horas con cincuenta y siete minutos; se registró vía Plataforma Nacional de Transparencia, la solicitud de información No. **271473900029424**, recibida en esta Unidad con fecha veintiuno de octubre del presente año; constante en 3 hojas original; mediante la que 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.**



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.**



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;**
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 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 e informar desde cuándo se implementó;**
34. **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;**
35. **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;**



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 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 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;**
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

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



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 de selección y asignación aleatoria de casos?

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

SEGUNDO: Visto lo anterior, y con fundamento en lo que establecen los artículos 6º y 8º de la Constitución Política de los Estados Unidos Mexicanos, 4º bis y 7º fracción IV, de la particular del estado de Tabasco, 49 y 50 fracción II de la Ley de Transparencia y Acceso a la Información Pública del estado de Tabasco; esta Unidad de Transparencia y Acceso a la Información, procede a tomar el siguiente: -----

----- **ACUERDO** -----

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



PRIMERO. Se tiene por recibida la solicitud de Información con folio No. **271473900029424**, de fecha veintiuno de octubre de dos mil veinticuatro mediante la solicitud referida y en apego a lo que establecen los artículos 6º y 8º de la Constitución General de la República, 4º bis y 7º fracción IV de la Constitución Política del estado libre y soberano de Tabasco, ha quedado registrada en esta Unidad en calidad de Solicitud de Información, bajo el folio No. **PJ/UTAIP/289/2024**; derivado de lo cual se procedió a integrar el expediente correspondiente.

SEGUNDO.- Se toma como medio para notificar y comunicar al particular los actos y resoluciones de esta autoridad jurídico administrativa la Plataforma Nacional de Transparencia.-----

TERCERO.- Con el fin de atender su requerimiento de información; la Unidad de Acceso, procedió a revisar puntualmente la solicitud; a fin de verificar si la misma; satisface lo establecido en el artículo 131 fracción II de la Ley de Transparencia y Acceso a la Información Pública, derivado de lo cual se advierte que la solicitud no satisface los requisitos establecidos por la Ley de Transparencia vigente en el Estado.-----

CUARTO.- Que de la revisión realizada por esta Unidad, a la presente solicitud se advierte que, su petición no cumple con los aspectos de claridad y precisión, toda vez que no hace alusión a *documento alguno específico en sus puntos*; se dice lo anterior, toda vez que el acceso a la información consiste en el derecho que tiene una persona de acceder a información generada, obtenida, adquirida, transformada, creada, administrada o en poder de los Sujetos Obligados o información de interés público, en los términos de la presente Ley; toda vez que, la información requerida por el peticionario resulta no ser clara, para su localización, por lo que esta Unidad de Transparencia, amablemente le requiere al solicitante para que aclare su solicitud, o sus preguntas, toda vez que el planteamiento de sus preguntas no son claras, para él o para las áreas que darán contestación a la información que requiere en su solicitud.

Se atiende lo anterior, de conformidad con los Criterio 03/17 y 19/10 emitidos por el Instituto Nacional de Transparencia y Acceso a la Información y Protección de Datos Personales, mismos que a la letra dicen:

Criterio 03/17

No existe obligación de elaborar documentos ad hoc para atender las solicitudes de acceso a la información.

Los artículos 129 de la Ley General de Transparencia y Acceso a la Información Pública y 130, párrafo cuarto, de la Ley Federal de Transparencia y Acceso a la Información Pública, señalan que los sujetos obligados deberán otorgar acceso a los documentos que se encuentren en sus archivos

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



o que estén obligados a documentar, de acuerdo con sus facultades, competencias o funciones, conforme a las características físicas de la información o del lugar donde se encuentre. Por lo anterior, los sujetos obligados deben garantizar el derecho de acceso a la información del particular, proporcionando la información con la que cuentan en el formato en que la misma obre en sus archivos; sin necesidad de elaborar documentos ad hoc para atender las solicitudes de información.

Criterio 19/10

No procede el trámite de solicitudes genéricas en el marco de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

En términos de lo establecido en el artículo 40 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, las solicitudes deben cumplir con determinadas características para que la autoridad esté en aptitud de identificar la atribución, tema, materia o asunto sobre lo que versa la solicitud de acceso a la información o los documentos de interés del particular. En ese sentido, tratándose de solicitudes genéricas, es decir, en las que no se describan los documentos a los que el particular requiera tener acceso, se considerará que se está en presencia de solicitudes presentadas fuera del marco de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, por lo que no procederá su trámite.

Lo anterior, siempre y cuando el solicitante no hubiese desahogado satisfactoriamente el requerimiento de información adicional efectuado por la autoridad con el objeto de allegarse de mayores elementos. Debe señalarse que el objetivo de la disposición citada es que las respuestas de las autoridades cumplan con las expectativas de los particulares al ejercer su derecho de acceso, por lo que se considera que éstos deben proporcionar elementos mínimos que permitan identificar la información requerida en razón de una atribución, tema, materia o asunto.

Expedientes:

- 2587/08 Comisión Federal de Telecomunicaciones – Juan Pablo Guerrero Amparán
- * 5568/09 Secretaría de Gobernación – Jacqueline Peschard Mariscal
- 5476/09 Comisión Federal de Mejora Regulatoria - Sigrid Arzt Colunga
- ** 1303/10 Instituto Federal de Acceso a la Información Pública – Sigrid Arzt Colunga
- 1324/10 Instituto Federal de Acceso a la Información Pública – Jacqueline Peschard Mariscal
- * Se aclara que la Comisionada Ponente correcta es María Elena Pérez-Jaén Zermeño.
- ** Se aclara que la Comisionada Ponente correcta es María Elena Pérez-Jaén

Por otra parte, de conformidad con lo establecido en el artículo sexto parte “**in fine**” de la Ley de Transparencia y Acceso a la Información Pública el Estado de Tabasco, que establece “**La información se proporcionará en el estado en que se encuentre. La obligatoriedad de los Sujetos Obligados de proporcionar información no comprende el procesamiento de la misma, ni el presentarla conforme al interés del solicitante, con excepción de la información que requiera presentarse en versión pública**” se hace del conocimiento del solicitante que deberá expresar de forma clara los documentos que requiere.



RESOLUCIÓN

PRIMERO.- Que con fecha veintiuno de octubre de dos mil veinticuatro, se registró en la Plataforma Nacional de Transparencia su solicitud de información con folio **271473900029424** y quedó registrada en esta Unidad bajo el folio **PJ/UTAIP/289/2024**.-----

SEGUNDO.- Que mediante los considerandos expuestos en este mismo documento, se le informan de manera clara y puntual las causas por las cuales resulta improcedente atender su solicitud de información en los términos que la ha presentado.-----

TERCERO.- Se le proporciona la orientación pertinente a fin de que se encuentre en posibilidad de presentar su solicitud de información conforme a lo que marca la legislación relativa y aplicable.-----

CUARTO.- *“Se le concede el término de diez días hábiles”* contados a partir de la recepción de este curso; a fin de que en este término subsane las observaciones que le han sido planteadas; *“y presente su solicitud de información, de manera clara y precisa”, para hacer factible la búsqueda del o los documentos deseados*, a fin de que pueda ser atendido, conforme a su derecho de acceso a la información.-----

QUINTO: Publíquese la solicitud recibida y la respuesta dada en el Portal de Transparencia de este Sujeto Obligado, como lo dispone el artículo 12 de los Lineamientos Generales para el Cumplimiento de las Obligaciones de Transparencia de los Sujetos Obligados en el Estado de Tabasco, para los efectos correspondientes. -----

Notifíquese al particular los actos de esta autoridad, a través de la Plataforma Nacional de Transparencia, medio indicado por el solicitante y en su oportunidad, archívese el presente asunto.-----Cúmplase-----

NOTIFÍQUESE Y CÚMPLASE. ASÍ LO ACUERDA, MANDA Y FIRMA, LA DIRECTORA DE LA UNIDAD DE TRANSPARENCIA Y ACCESO A LA INFORMACION DEL PODER JUDICIAL DEL ESTADO DE TABASCO, A LOS VEINTINUEVE DIAS DEL MES DE OCTUBRE DE DOS MIL VEINTICUATRO.-----CONSTE.

Esta hoja de firmas corresponde al Acuerdo de Prevención de fecha 29 de octubre de 2024, dictado en el expediente relativo a la solicitud de información identificada con el número de folio 271473900029424.-----

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