



"2024, Año de Felipe Carrillo Puerto, Benemérito del Proletariado,
Revolucionario y Defensor del Mayab"
"Nuestro Poder Judicial, puerta de acceso a la justicia
y garante de la paz social"



UNIDAD DE TRANSPARENCIA Y ARCHIVO

FOLIO PNT: **040086300019524**

RESOLUCIÓN: **55/UT/24-2025**

SOLICITUD: **PJE-UT-3182**

ESTIMADO SOLICITANTE

P R E S E N T E.-

**UNIDAD DE TRANSPARENCIA DEL PODER JUDICIAL DEL ESTADO DE CAMPECHE,
CASA DE JUSTICIA; SAN FRANCISCO DE CAMPECHE, CAMPECHE, A SEIS DE
NOVIEMBRE DEL DOS MIL VEINTICUATRO.**

ANTECEDENTES

1. CONTENIDO DE LA SOLICITUD. A través de la Plataforma Nacional de Transparencia, mediante la cual requirió lo siguiente:

"... Mismo que por economía procesal, se tiene por reproducida como si a la letra se insertase a la presente solicitud con número de folio 040086300019524. ..."

2. FECHA DE PRESENTACIÓN DE LA SOLICITUD. Dicha solicitud de acceso a la información se tuvo como legalmente admitida al día siguiente de su presentación. Con fundamento en el artículo 130 de la Ley de Transparencia y Acceso a la Información del Estado de Campeche.

3. TRÁMITE DE BÚSQUEDA DE INFORMACIÓN. Se solicitó a través de oficio número 89/UT/24-2025, dirigido a la Dirección de Tecnologías de la Información del Poder Judicial del Estado, a fin de que solventará la información solicitada.

4. SOLVENTACIÓN DE LA INFORMACIÓN. En virtud de lo anterior se tuvo por recibido el oficio número 102/DRM/24-2025, suscrito por el Licenciado Guadalupe Ismael Pech Balán, Director Interino de Tecnologías de la Información del Poder Judicial del Estado de Campeche.



UNIDAD DE TRANSPARENCIA Y ARCHIVO

CONSIDERACIONES

I. COMPETENCIA. Esta Unidad de Transparencia del Poder Judicial del Estado es **COMPETENTE** para conocer y resolver la presente petición, tal y como lo establecen los artículos 3, fracción XXII, 45, fracciones II y XIV, 50, 51, fracción II, y 125 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Campeche; 293 y 295 de la Ley Orgánica del Poder Judicial del Estado de Campeche; y fracción III del artículo 201 del Reglamento Interior General del Poder Judicial del Estado de Campeche.

II. FUNDAMENTO LEGAL PARA SU RESPUESTA. Por disposición de los artículos 3, 44, 134 y 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Campeche, en relación con los artículos 6 y 16 de la Constitución Política de los Estados Unidos Mexicanos, toda solicitud de acceso a la información pública debe ser contestada mediante resolución escrita, fundada y motivada, por medio de la cual se conceda o niegue, en su caso, la información requerida.

III. ENTREGA DE LA INFORMACIÓN¹: La modalidad elegida por Usted fue: Correo electrónico e independiente de su envío, la respuesta se subirá al sistema de solicitudes de acceso a la información de la PNT.

IV. RESPUESTA.

Sección 1.

| Cuestionamiento | Respuesta |
|--|--|
| 1. Informar si dentro de la institución se cuenta con un gobierno de seguridad de la información o Ciberseguridad y cuáles áreas participan; | Se cuenta con políticas de seguridad de la información, mismas que se han establecidos en todas las sedes del Poder Judicial. |
| 2. Señalar si se cuenta con lo siguiente: a) Un marco de mejores prácticas aplicables a la gestión de las TIC en los | a) Como parte de los planes de seguridad informática, se han establecidos políticas de seguridad de la |

¹ Artículo 137 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Campeche.



UNIDAD DE TRANSPARENCIA Y ARCHIVO

| | |
|--|--|
| <p>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;</p> <p>b) Informar sí se cuenta con un Inventario Institucional de bienes y servicios de TIC;</p> <p>c) Un plan de continuidad de operaciones, y señalar la fecha de implementación;</p> <p>d) Informar sí se ha desarrollado e implementado el plan de recuperación ante desastres, señalar la fecha de desarrollo e implementación;</p> <p>e) Desarrollado e implementado un programa de gestión de vulnerabilidades;</p> <p>f) Marco de Gestión de Seguridad de la Información (MGSI) o Sistema de Gestión de Seguridad de la Información (SGSI);</p> <p>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;</p> <p>h) Informar sí se cuenta con un diagnóstico de identificación de los procesos y activos esenciales de la Institución;</p> <p>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.</p> | <p>información en la gestión de las TIC. Estas se han aplicado en la Red de Seguridad Perimetral.</p> <p>b) Si se cuenta.</p> <p>c) Si se cuenta con un plan de continuidad de las operaciones.</p> <p>d) Si se ha desarrollado e implementando el plan de recuperación de desastres. Implementado desde mayo del 2016.</p> <p>e) Si se ha desarrollado e implementando el programa de gestión de vulnerabilidades.</p> <p>f) Si se ha desarrollado e implementando un Sistema de Gestión de la Seguridad de la Información.</p> <p>g) Si se ha desarrollado e implementando una política general de seguridad de la información, y quienes intervienen, es el personal de la Dirección de Tecnologías de la Información. Esta política se estableció desde Implementado desde mayo del 2016.</p> <p>h) Si se cuenta con un diagnóstico de la situación actual de las Tecnologías de Información en el Poder Judicial.</p> <p>i) Se cuenta con personal técnico capacitación, así como la infraestructura tecnológica para atender Incidentes de Seguridad de la Información.</p> |
| <p>3.- Informar sí es que se cuenta con una estrategia de Ciberseguridad dentro de la institución, en caso de respuesta afirmativa, informar lo siguiente:</p> | <p>Si se cuenta con una estrategia de Ciberseguridad.</p> <p>i. La fecha de creación fue 14 de enero del 2015</p> |



UNIDAD DE TRANSPARENCIA Y ARCHIVO

| | |
|--|---|
| <ul style="list-style-type: none">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; | <ul style="list-style-type: none">ii. La fecha de implementación fue 14 de enero del 2015iii. Si se ha actualizado al menos en tres ocasiones.iv. La dirección de Tecnologías de la Información. |
| 4.- Informar si se emplea la firma electrónica avanzada en la institución; | Sí se cuenta. |
| 5.- Informar si se realizan simulacros sobre el plan de recuperación de desastres o en caso de incidentes cibernéticos; | No. |
| 6.- Señalar si se cuentan con lineamientos de programación y desarrollo de sistemas informáticos seguros; | No se cuenta con lineamientos documentados. |
| 7.- Informar si los servicios de centros de datos son propios, de otra institución gubernamental o de un tercero; | Propios |
| 8.- Informar si para el trabajo remoto se cuentan con lineamientos de seguridad para las video llamadas; | Si 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: <ul style="list-style-type: none">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; | Sí se cuenta <ul style="list-style-type: none">a) SIc) Si se cuenta con un control institucional del total de los correos contenidos en las carpetas de usuarios.d) Si se cuenta con una solución de filtrado para el correo no deseado o correo no solicitado, así como programas informáticos, que protegen del envío y recepción de correos electrónicos maliciosos.e) Si se cuenta con el cifrado en el envío de información. |



UNIDAD DE TRANSPARENCIA Y ARCHIVO

| | |
|---|---|
| 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; | Sí se cuenta. |
| 11.- Informar si la página web de la institución cuenta con: a) Aviso de privacidad b) Certificados digitales vigentes | a) Si se cuenta b) Si se cuenta |
| 12. Informar si el personal responsable se ha capacitado en la implementación del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos; | No |
| 13. Informar si se cuentan con: a) Los mecanismos de supervisión y evaluación que permitan medir la efectividad de los controles de seguridad de la información; b) Indicadores que permitan medir la madurez institucional en la gestión de seguridad de la información; | a) No. b) No. |
| 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. |
| 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?; | No se cuenta. |
| 16.- Informar si se cuenta con un modelo o sistema de comunicación, para informar a la sociedad en general sobre los eventos o | No se cuenta con un modelo o sistema de comunicación, para informar a la sociedad en general sobre los eventos o incidentes de |



UNIDAD DE TRANSPARENCIA Y ARCHIVO

| | |
|--|---|
| 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; | seguridad de la institución. |
| 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; | No 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. |
| 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 se cuenta con lineamientos para el traslado de activos físicos 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: a) Transparencia; b) Protección de datos personales; c) Archivos públicos; o, d) Seguridad de la información. | a) No b) No c) No d) No |
| 20.- Informar si han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas; | Sí se ha tenido. Tres brechas. |
| 21.- Informar si se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son; Si se han adoptado este tipo de esquemas. Por ejemplo: <ul style="list-style-type: none">Control de acceso por medio de nombre de usuario y contraseña.Protocolo HTTPS y Certificados SSL vigentes.Anonimización de datos en las sentencias públicas.Almacenamiento de información en bases de datos con | Si se han adoptado esquemas de mejores prácticas en materia de protección de datos personales, entre los que podemos mencionar: <ul style="list-style-type: none">Control de acceso por medio de nombre de usuario y contraseña.Protocolo HTTPS y Certificados SSL vigentes. |



UNIDAD DE TRANSPARENCIA Y ARCHIVO

| | |
|--|--|
| <p>acceso únicamente a personal autorizado.</p> <ul style="list-style-type: none">• Segmentación de la RED interna.• Implementación de Seguridad Perimetral en la Red Interna (FIREWALL). | <ul style="list-style-type: none">• Almacenamiento de información en bases de datos con acceso únicamente a personal autorizado.• Segmentación de la RED interna.• Implementación de Seguridad Perimetral en la Red Interna (FIREWALL). |
| <p>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;</p> | <p>R. Sí implica tratamiento relevante de datos personales. No se tiene registro de evaluaciones de impacto.</p> |
| <p>23.- Informar si se cuenta con documento de seguridad en materia de protección de datos personales; DERECHOS HUMANOS</p> | <p>No se cuenta.</p> |
| <p>24.- Informar si se cuenta con un plan de comunicación institucional en caso de un incidente de ciberseguridad o seguridad de la información;</p> | <p>No se cuenta.</p> |
| <p>25.- Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución;</p> | <p>Estas políticas se actualizan al menos una vez al año.</p> |
| <p>26.- Informar si se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad;</p> | <p>No se llevan auditorías externas, pero si se hacen auditorías internas, al menos una vez al año.</p> |
| <p>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.</p> | <p>Sí se cuenta. Es interno.</p> |



UNIDAD DE TRANSPARENCIA Y ARCHIVO

| | |
|---|----------------------|
| 28.- Señalar sí las páginas web de los buscadores de versiones públicas de sentencias del Tribunal, tienen certificados digitales vigentes. | Sí se cuenta. |
|---|----------------------|

Sección 2

| Cuestionamiento | Respuesta |
|--|--|
| 29.- Informar sí dentro de la institución se cuenta con un gobierno de seguridad de la información o ciberseguridad y cuáles áreas participan; | Se cuenta con políticas de seguridad de la información, mismas que se han establecidos en todas las sedes del Poder Judicial. |
| 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; | Si se cuenta con una estrategia de ciberseguridad i. La fecha de creación fue 14 de enero del 2015 ii. La fecha de creación fue 14 de enero del 2015 iii. Si se ha actualizado al menos en tres ocasiones iv. La dirección de Tecnologías de la Información |
| 31.- Informar sí se cuenta con un sistema de gestión de seguridad de la información dentro de la institución; | Si se cuenta con un sistema de gestión de la 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?; ...". | NO se cuenta. |

Finalmente, en caso de no estar conforme con esta respuesta, puede interponer un **RECURSO DE REVISIÓN**, a través de la Plataforma Nacional de Transparencia, en la dirección electrónica:



"2024, Año de Felipe Carrillo Puerto, Benemérito del Proletariado,
Revolucionario y Defensor del Mayab"
"Nuestro Poder Judicial, puerta de acceso a la justicia
y garante de la paz social"



UNIDAD DE TRANSPARENCIA Y ARCHIVO

<https://www.plataformadetransparencia.org.mx/>; contando con un plazo de quince días hábiles posteriores a la notificación de la presente.

Ahora bien, si tiene alguna duda, puede llamar al número telefónico 9818117757, o bien, puede acudir directamente a la Unidad de Transparencia y Archivo del Poder Judicial, ubicada Avenida Héroes de Nacozari, con Avenida Colosio número 03, colonia Cuatro Caminos, código postal 24070, San Francisco de Campeche, Campeche, en un horario de 8:30 a 15:00 horas; o, si requiere mayor información, puede enviar un correo a la siguiente dirección: transparencia@poderjudicialcampeche.gob.mx
En mérito de lo anterior, se:

RESUELVE

PRIMERO. - Se **OTORGA** el acceso a la información que el Poder Judicial del Estado de Campeche, está obligado a cumplir por las disposiciones legales aplicables en relación a la solicitud marcada con el número de folio: **040086300019524**, y número de control interno de esta Unidad **PJE-UT-3182**, conforme a la información solicitada.

SEGUNDO. - Se tiene como resuelta la solicitud de Acceso a la Información Pública solicitud marcada con el número de folio: **040086300019524**, y número de control interno de esta Unidad **PJE-UT-3182**, en términos de lo resuelto en el punto IV de las Consideraciones de la presente.

TERCERO.- Hágase saber al solicitante que en caso de considerar que la respuesta a su solicitud de información no ha sido en apego a los principios de legalidad y seguridad jurídica, puede interponer ante la Comisión de Transparencia y Acceso a la Información Pública del Estado de Campeche, el Recurso de Revisión previsto en el Título Noveno de la Ley de Transparencia y Acceso a la Información Pública del Estado de Campeche, dentro del término de quince días hábiles posteriores a la notificación de la presente.



"2024, Año de Felipe Carrillo Puerto, Benemérito del Proletariado,
Revolucionario y Defensor del Mayab"
"Nuestro Poder Judicial, puerta de acceso a la justicia
y garante de la paz social"



UNIDAD DE TRANSPARENCIA Y ARCHIVO

CUARTO. - Notifíquese la respuesta al solicitante, mediante la forma indicada en el punto III de las Consideraciones de la misma.

ATENTAMENTE



**DRA. BRENDA GABRIELA MEDINA ATUN.
SUBDIRECTORA EN FUNCIONES DE COORDINADORA
DE LA UNIDAD DE TRANSPARENCIA Y ARCHIVO
DEL PODER JUDICIAL DEL ESTADO DE CAMPECHE.**