Morelia, Michoacán a 25 de noviembre de 2024
Solicitud de Información: 160353224000046
Expediente Interno: TEEM-UT-SAIP-042/2024
Asunto: Se emite respuesta

C. Solicitante
P R E S E N T E

En atención a su solicitud recibida mediante Plataforma Nacional de Transparencia, me permito informarle que, dando cabal cumplimiento a las funciones que se establecen en el artículo 126 fracciones II, IV y V de la Ley de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Michoacán de Ocampo[1], se remitió el folio correspondiente, mediante el oficio número **TEEM-TRANS-141/2024, a la Secretaría de Administración, a la Unidad de Sistemas, así como a la Oficialía de Datos Personales,** todas de este Tribunal Electoral, al ser las áreas que con base en sus facultades, competencias y funciones, pudieran contar con la información:

Solicitud de información con número de folio: **160353224000046**

Información solicitada:

"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*

[1] En adelante *Ley Estatal de Transparencia.*

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 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 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)" (SIC)

***Medio para recibir notificaciones:** Sistema de Solicitudes de Información de la Plataforma Nacional de Transparencia*
***Medio de Entrega:** Electrónico a través del Sistema de Solicitudes de Acceso a la Información de la PNT*
***Nota:** Contiene "Documentación anexada"*

La **Oficialía de Datos Personales**, remitió su respuesta el día doce de noviembre del año en curso, a través del oficio número **TEEM-UTDP-059/2024**, el cual se adjunta para su consulta o reproducción.

El día veintiuno de noviembre del año que transcurre, a través del oficio número **TEEM-TRANS-161/2024**, esta Unidad de Transparencia consideró necesario requerir nuevamente a la **Secretaría de Administración y Unidad de Sistemas**, a fin de que dieran atención a la Solicitud de Acceso a la Información con número de folio 160353224000046, a más tardar el día veintidós de noviembre de dos mil veinticuatro; lo anterior a efecto de poder estar en condiciones de cumplir con lo dispuesto por el artículo 75 de la *Ley Estatal de Transparencia*, respecto a la fecha límite para dar respuesta a dicha solicitud.

Atento a lo anterior, los días veintidós y veinticinco de noviembre del año en curso, las áreas anteriormente señaladas, dieron respuesta a su solicitud de información; en tal virtud, **se adjuntan los oficios número TEEM-SA-224/2024 y TEEM-SIS-038-2024**, para su consulta o reproducción.

Notifíquese al solicitante a través de la Plataforma Nacional de Transparencia, en términos del artículo 67, párrafo primero, de la *Ley Estatal de Transparencia*, en virtud de que señaló como Medio para recibir notificaciones: Sistema de Solicitudes de Información de la Plataforma Nacional de Transparencia.

Por otra parte, en caso de que tenga problemas para visualizar la respuesta, se puede comunicar al teléfono 443 113 01 30, extensión 140, con la titular de la Unidad de Transparencia, o bien, a la siguiente dirección electrónica: transparenciateem@gmail.com

Finalmente, le informo que en términos del numeral 135 de la *Ley Estatal de Transparencia*, el solicitante podrá presentar recurso de revisión, ante el organismo garante, dentro de los quince días siguientes a la fecha de la notificación de la respuesta.

Se emite la presente, con fundamento en los artículos 1, 2, 9, 64 y 75 de la *Ley Estatal de Transparencia*.

Atentamente

TRIBUNAL ELECTORAL DEL ESTADO
UNIDAD DE TRANSPARENCIA

Lic. Juana María López Zepahua
Jefa de Departamento "A" de Transparencia
del Tribunal Electoral del Estado

TEEMICH
TRIBUNAL ELECTORAL DEL ESTADO
MICHOACÁN

Oficialía de datos
23-OCT-2024
11:45

SISTEMAS INFORMÁTICOS
23 OCT. 2024
TRIBUNAL ELECTORAL DEL ESTADO DE MICHOACÁN
Hora: 11:37

RECIBIDO
11:36 hrs
23 OCT 2024
DEPARTAMENTO DE RECURSOS HUMANOS

Morelia, Michoacán a 23 de octubre de 2024
Oficio: TEEM-TRANS-141/2024
Asunto: Se remite Acuerdo de recepción y turno a fin de dar respuesta a la Solicitud de Acceso a la Información con número de folio 160353224000046, radicada bajo el número de expediente TEEM-UT-SAIP-042/2024

Mtro. Arturo Ángel Parra Luviano
Secretario de Administración;
M.E. Edgar Abdiel Barriga Delgado
Jefe de la Unidad de Sistemas;
Lic. Jorge Torres Reyes
Oficial de Datos Personales;
todos del Tribunal Electoral del Estado
Presente

RECURSOS MATERIALES
23 OCT. 2024
TRIBUNAL ELECTORAL DEL ESTADO DE MICHOACÁN
Hora: 11:37

SECRETARÍA DE ADMINISTRACIÓN
23 OCT. 2024
TRIBUNAL ELECTORAL DEL ESTADO DE MICHOACÁN
Hora: 11:20

11:48 hrs

Con fundamento en los artículos 74 de la Ley de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Michoacán de Ocampo y 87 fracción I del Reglamento del Tribunal Electoral del Estado de Michoacán, de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, y en atención al punto SÉPTIMO del ACUERDO DE INICIO Y TURNO de fecha veintitrés de octubre de dos mil veinticuatro, dictado dentro del Expediente: TEEM-UT-SAIP-042/2024, se remite dicho proveído y anexo, a fin de que las áreas a su cargo, den respuesta a la Solicitud de Acceso a la Información presentada por un particular el día veintiuno de octubre del año en curso.

Lo anterior, al ser las áreas que, conforme a lo dispuesto por los artículos 80 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo; 60, 61, 64, 76, 87 y demás relativos y aplicables del Reglamento Interior del Tribunal Electoral del Estado, pueden contar con la información requerida de acuerdo con sus facultades, competencias y funciones, por lo que solicito de su valiosa colaboración a efecto de que tengan a bien realizar una búsqueda exhaustiva y razonable de la información requerida y remitan sus respuestas a esta Unidad de Transparencia conforme a lo señalado en el ACUERDO DE INICIO Y TURNO adjunto.

Sin más por el momento, me despido.

Atentamente

RECIBIDO
23 OCT. 2024
11:47 Jessi
PRESIDENCIA
TRIBUNAL ELECTORAL DEL ESTADO

Lic. Juana María López Zepahua
Jefa de Departamento "A" de Transparencia
del Tribunal Electoral del Estado

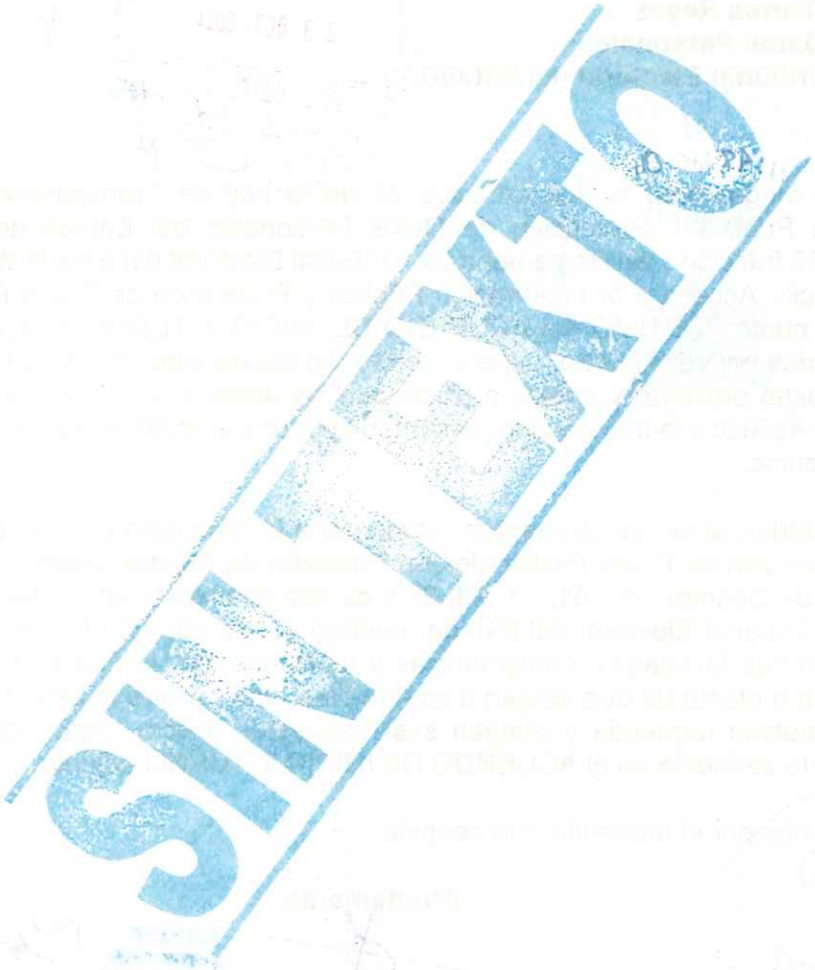
RECIBIDO
23 OCT. 2024
PONENCIA MAGISTRADA YOLANDA CAMACHO OCHOA
11:47

TRIBUNAL ELECTORAL DEL ESTADO
UNIDAD DE TRANSPARENCIA

RECIBIDO
11:50
23 OCT. 2024
PONENCIA MAGISTRADA YURISHA ANDRADE MORALES

ACUSE

C.c.p. Dra. Yurisha Andrade Morales. Magistrada Presidenta del Tribunal Electoral del Estado.
C.c.p. Dra. Alma Rosa Bahena Villalobos. Magistrada del Tribunal Electoral del Estado.
C.c.p. Lcda. Yolanda Camacho Ochoa. Magistrada del Tribunal Electoral del Estado.
C.c.p. Dr. Salvador Alejandro Pérez Contreras. Magistrado del Tribunal Electoral del Estado.
C.c.p. Lic. Julio César Martínez Villagómez y José Hernández Tadeo. Jefe de Departamento de Recursos Humanos y Recursos Materiales, respectivamente.


SIN TEXTO

Morelia, Michoacán a 23 de octubre de 2024
EXPEDIENTE INTERNO: TEEM-UT-SAIP-042/2024

ACUERDO DE INICIO Y TURNO

Vista la Solicitud de Acceso a la Información Pública presentada por un particular a través del Sistema de Solicitudes de Acceso a la Información[1] de la Plataforma Nacional de Transparencia[2], registrada con el número de folio **160353224000046**, con fecha oficial de presentación veintiuno de octubre de dos mil veinticuatro; la Unidad de Transparencia del Tribunal Electoral del Estado[3], acuerda:

PRIMERO. – El Tribunal Electoral del Estado[4] es COMPETENTE formalmente para conocer de la Solicitud de Acceso a la Información con número de folio **160353224000046**, de conformidad con lo establecido por los artículos 8, 77 y demás relativos y aplicables de la Ley de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Michoacán de Ocampo[5].

SEGUNDO. – Para la atención de la presente Solicitud de Acceso a la Información, deberá tenerse en cuenta el horario de labores y días hábiles de este órgano jurisdiccional, así como el calendario de días hábiles del Instituto Michoacano de Transparencia, Acceso a la Información y Protección de Datos Personales[6].

TERCERO. – Fórmese y regístrese el expediente con clave alfanumérica **TEEM-UT-SAIP-042/2024**, relativo a la **Solicitud de Acceso a la Información Pública** con número de folio **160353224000046**, en la cual se solicita lo siguiente:

"APARTADO 1

---

[1] SISAI 2.0.
[2] *PNT.*
[3] En adelante *Unidad de Transparencia.*
[4] En lo sucesivo *Tribunal Electoral.*
[5] En lo subsecuente *Ley Estatal de Transparencia.*
[6] Este último es consultable en: https://imaip.org.mx/box/via/plataforma/CalendarioIMAIP2024.pdf

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 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 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)" (SIC)

Medio para recibir notificaciones: *Sistema de Solicitudes de Información de la Plataforma Nacional de Transparencia*
Medio de Entrega: *Electrónico a través del Sistema de Solicitudes de Acceso a la Información de la PNT*
Nota: *Contiene "Documentación anexada"*

CUARTO. – Con fundamento en los artículos 74 de la *Ley Estatal de Transparencia*; 80 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo; 87 fracción I del Reglamento del Tribunal Electoral del Estado de Michoacán, de Transparencia, Acceso a la Información

Pública y Protección de Datos Personales[7]; 60, 61, 64, 76, 87 y demás relativos y aplicables del Reglamento Interior del Tribunal Electoral del Estado[8], **se turna la presente solicitud de información a la Secretaría de Administración, a la Unidad de Sistemas así como a la Oficialía de Datos Personales – Unidad de Transparencia, todas de este *Tribunal Electoral,*** a fin de que proporcionen a esta *Unidad de Transparencia* la información correspondiente a la solicitud de acceso, transcrita en el punto anterior.

QUINTO. – Toda vez que la solicitud de mérito engloba diversas áreas, para la atención de esta se solicita:

I. Que la Secretaría de Administración, atienda lo referente a:

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;

b) informar si se cuenta con un 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.

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.

---

[7] En lo sucesivo *Reglamento de Transparencia del Tribunal Electoral.*

[8] En adelante *Reglamento Interior.*

38. Informar si se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos;
39. 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.

II. Que la Unidad de Sistemas, atienda lo referente a:

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 si se cuenta con lo siguiente:

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.
11. Informar si la página web de la institución cuenta con: b) certificados digitales vigentes;

12. Informar si el personal responsable se ha capacitado en la implementación del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos;
13. Informar si se cuentan con: a) Los mecanismos de supervisión y evaluación que permitan medir la efectividad de los controles de seguridad de la información; b) Indicadores que permitan medir la madurez institucional en la gestión de seguridad de la información;
14. Informar si dentro de la institución se cuenta con un Programa de formación en la cultura de la seguridad de la información o de ciberseguridad; y en caso afirmativo señalar: cuándo se implementó;
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 participan? e informar desde cuándo se implementó;
20. Informar si han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas;
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;
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;
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;
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;
36. Informar si 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 si 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;

40. Informar si han tenido brechas de ciberseguridad desde el año 2014 a la fecha de la presente solicitud y señalar cuántas;
41. Informar si 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;
44. Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución;
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;
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?

III. Que la Oficialía de Datos Personales – Unidad de Transparencia, atienda lo referente a:

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;

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?;
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;
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;
26. Informar si se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad;
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?;
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;
42. Informar si se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son;
43. 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;
45. Informar si se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad.

SEXTO. – Lo anterior, lo deberán notificar y/o remitir a esta *Unidad de Transparencia* dentro de los términos previstos por las respectivas fracciones del artículo 87 del *Reglamento de Transparencia del Tribunal Electoral*, que señala que

el procedimiento interno de gestión de solicitud se desahogará conforme lo siguiente:

Hipótesis	Días hábiles	Fecha para notificar y/o remitir a la *Unidad de Transparencia*
Fracción III. En caso de que la información solicitada sea pública y obre en los archivos del área.[9]	Al día hábil siguiente a aquél en que hayan recibido la solicitud.	24 de octubre
Fracción IV. Si la información solicitada se encuentra clasificada como temporalmente reservada o confidencial.[10]	Cinco días hábiles, contados a partir de que recibió la solicitud de acceso a la información por conducto de la Unidad de Transparencia.	29 de octubre
Fracción V. En caso de que la información solicitada contenga partes o secciones clasificadas como temporalmente reservadas o confidenciales.[11]	Cinco días hábiles siguientes a aquél en que haya recibido la solicitud de acceso a la información.	30 de octubre
Fracción VII. Cuando la información solicitada no se encuentre en los archivos del área, ya sea por inexistencia o incompetencia que no sea notoria.[12]	Cinco días hábiles siguientes contados a partir de que haya recibido la solicitud por parte de la Unidad.	29 de octubre

[9] La notificación que el área envíe a la Unidad de Transparencia debe precisar, en su caso, los costos de reproducción y envío de acuerdo con las diversas modalidades que contemplan las secciones SÉPTIMA y OCTAVA del *Reglamento de Transparencia del Tribunal Electoral*, o bien la fuente, lugar y forma en que se puede consultar, reproducir o adquirir.

[10] El titular del área responsable deberá remitir al Comité de Transparencia la solicitud y un oficio en el que funde y motive dicha clasificación, así como el expediente correspondiente, para que el Comité de Transparencia resuelva si: a) Confirma la clasificación; b) Modifica la clasificación y ordena la entrega de una versión pública de la información solicitada; o, c) Revoca la clasificación y concede el acceso a la información.

[11] El área correspondiente deberá remitir al Comité de Transparencia, un oficio que funde y motive su clasificación aplicando la prueba de daño a que se refiere el artículo 28 del *Reglamento de Transparencia del Tribunal Electoral*, así como de la versión pública del documento, para los efectos referidos en la fracción IV del artículo 87 del supracitado reglamento, y una muestra del documento en su versión original.

[12] El área deberá remitir al Comité de Transparencia, por conducto de la Unidad de Transparencia, la solicitud, un informe fundado y motivado donde se expongan las gestiones que realizó para la ubicación de la información, conforme a lo siguiente: a) Motivar y precisar las razones por las que se buscó la información en determinadas áreas; b) Los criterios de búsqueda utilizados; y, c) Las demás circunstancias que fueron tomadas en cuenta.

No omito manifestarle que, en caso de no encuadrar en ninguna de las hipótesis anteriores, se les solicita que, en el término de cinco días hábiles siguientes a aquél en que hayan recibido la solicitud de acceso a la información, remitan su respuesta a esta *Unidad de Transparencia*, en virtud de que el artículo 86 del *Reglamento de Transparencia del Tribunal Electoral*, señala que la respuesta a la solicitud deberá ser notificada al interesado en el menor tiempo posible, que no podrá ser mayor de veinte días hábiles, contados a partir del día hábil siguiente al de la presentación.

SÉPTIMO. – Gírese el presente proveído al área correspondiente, en cumplimiento al artículo 74 de la *Ley Estatal de Transparencia*, y anéxese ACUSE DE RECIBO DE SOLICITUD DE INFORMACIÓN con número de folio 160353224000046 y documentación anexada, para mayor precisión.

Así lo acordó la Jefa de Departamento "A" de Transparencia del Tribunal Electoral del Estado, con fundamento en los artículos 64, 75, 77 y 79 de la Ley de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Michoacán de Ocampo, y 70, 78, 85 y 86 del Reglamento del Tribunal Electoral del Estado de Michoacán, de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.

Atentamente

TRIBUNAL ELECTORAL DEL ESTADO
UNIDAD DE TRANSPARENCIA

Lic. Juana María López Zepahua
Jefa de Departamento "A" de Transparencia
del Tribunal Electoral del Estado

TEEMICH

TRIBUNAL ELECTORAL DEL ESTADO
MICHOACÁN

Morelia, Michoacán a 23 de octubre de 2024
Oficio: TEEM-TRANS-142/2024
Asunto: Se remite oficio en alcance al Acuerdo de recepción y turno de la Solicitud de Acceso a la Información con número de folio 160353224000046, radicada bajo el número de expediente TEEM-UT-SAIP-042/2024

M.E. Edgar Abdiel Barriga Delgado
Jefe de la Unidad de Sistemas
de! Tribunal Electoral del Estado
Presente

Con fundamento en los artículos 74 de la Ley de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Michoacán de Ocampo; 87 fracción I del Reglamento del Tribunal Electoral del Estado de Michoacán, de Transparencia, Acceso a la Información Pública y Protección de Datos Personales[1]; y conforme a los principios de exhaustividad y congruencia que deben imperar en materia de acceso a la información[2], me permito exponer lo siguiente:

Que en atención a la **Solicitud de Acceso a la Información con número de folio 160353224000046**, presentada por un particular el día veintiuno de octubre del año en curso y radicada bajo el número de expediente: **TEEM-UT-SAIP-042/2024**, solicito que, **adicional a los puntos turnados por medio del oficio TEEM-TRANS-141/2024, el área a su cargo también dé respuesta a los siguientes puntos:**

> *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;*
> *b) informar si se cuenta con un 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.*

ACUSE

SISTEMAS INFORMÁTICOS
23 OCT. 2024
TRIBUNAL ELECTORAL DEL ESTADO DE MICHOACÁN
Hora: 15:46

[1] En adelante *Reglamento de Transparencia del Tribunal Electoral.*
[2] Los sujetos obligados al responder una solicitud de acceso a la información deben cumplir con estos principios. La congruencia implica que la respuesta debe coincidir con el requerimiento del particular y la exhaustividad implica que la respuesta debe referirse a cada uno de los puntos solicitados.

Lo anterior, lo deberá notificar y/o remitir a esta *Unidad de Transparencia* dentro de los términos previstos por las respectivas fracciones del artículo 87 del *Reglamento de Transparencia del Tribunal Electoral*, que señala que el procedimiento interno de gestión de solicitud se desahogará conforme lo siguiente:

Hipótesis	Días hábiles	Fecha para notificar y/o remitir a la *Unidad de Transparencia*
Fracción III. En caso de que la información solicitada sea pública y obre en los archivos del área.[3]	Al día hábil siguiente a aquél en que hayan recibido la solicitud.	24 de octubre
Fracción IV. Si la información solicitada se encuentra clasificada como temporalmente reservada o confidencial.[4]	Cinco días hábiles, contados a partir de que recibió la solicitud de acceso a la información por conducto de la Unidad de Transparencia.	29 de octubre
Fracción V. En caso de que la información solicitada contenga partes o secciones clasificadas como temporalmente reservadas o confidenciales.[5]	Cinco días hábiles siguientes a aquél en que haya recibido la solicitud de acceso a la información.	30 de octubre
Fracción VII. Cuando la información solicitada no se encuentre en los archivos del área, ya sea por inexistencia o incompetencia que no sea notoria.[6]	Cinco días hábiles siguientes contados a partir de que haya recibido la solicitud por parte de la Unidad.	29 de octubre

[3] La notificación que el área envíe a la Unidad de Transparencia debe precisar, en su caso, los costos de reproducción y envío de acuerdo con las diversas modalidades que contemplan las secciones SÉPTIMA y OCTAVA del *Reglamento de Transparencia del Tribunal Electoral*, o bien la fuente, lugar y forma en que se puede consultar, reproducir o adquirir.

[4] El titular del área responsable deberá remitir al Comité de Transparencia la solicitud y un oficio en el que funde y motive dicha clasificación, así como el expediente correspondiente, para que el Comité de Transparencia resuelva si: a) Confirma la clasificación; b) Modifica la clasificación y ordena la entrega de una versión pública de la información solicitada; o, c) Revoca la clasificación y concede el acceso a la información.

[5] El área correspondiente deberá remitir al Comité de Transparencia, un oficio que funde y motive su clasificación aplicando la prueba de daño a que se refiere el artículo 28 del *Reglamento de Transparencia del Tribunal Electoral*, así como de la versión pública del documento, para los efectos referidos en la fracción IV del artículo 87 del supracitado reglamento, y una muestra del documento en su versión original.

[6] El área deberá remitir al Comité de Transparencia, por conducto de la Unidad de Transparencia, la solicitud, un informe fundado y motivado donde se expongan las gestiones que realizó para la ubicación de la información,

Lo anterior, en el entendido de que, en caso de no encuadrar en ninguna de las hipótesis precisadas, se le solicita que, en el término de cinco días hábiles siguientes a aquél en que haya recibido la solicitud de acceso a la información, remita su respuesta a esta *Unidad de Transparencia*, en virtud de que el artículo 86 del *Reglamento de Transparencia del Tribunal Electoral*, señala que la respuesta a la solicitud deberá ser notificada al interesado en el menor tiempo posible, que no podrá ser mayor de veinte días hábiles, contados a partir del día hábil siguiente al de la presentación.

Lo anterior, al ser el área que, conforme a lo dispuesto por los artículos 60, 61 y demás relativos y aplicables del Reglamento Interior del Tribunal Electoral del Estado, puede contar con la información requerida de acuerdo con sus facultades, competencias y funciones, por lo que solicito de su valiosa colaboración a efecto de que tenga a bien realizar una búsqueda exhaustiva y razonable de la información requerida y remita su respuesta a esta Unidad de Transparencia dentro de los plazos señalados en el recuadro anteriormente inserto.

Sin más por el momento, me despido.

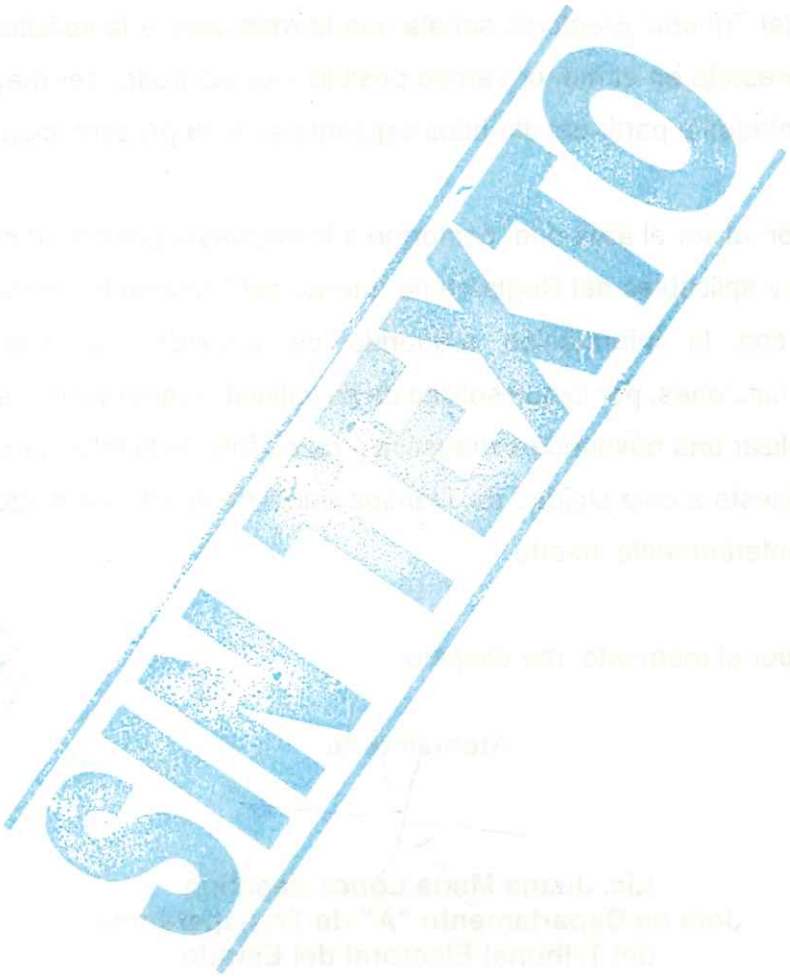
Atentamente

TRIBUNAL ELECTORAL DEL ESTADO
UNIDAD DE TRANSPARENCIA

Lic. Juana María López Zepahua
Jefa de Departamento "A" de Transparencia
del Tribunal Electoral del Estado

---

conforme a lo siguiente: a) Motivar y precisar las razones por las que se buscó la información en determinadas áreas; b) Los criterios de búsqueda utilizados; y, c) Las demás circunstancias que fueron tomadas en cuenta.


SIN TEXTO

MORELIA, MICHOACÁN A 12 DE NOVIEMBRE DE 2024.
OFICIO: **TEEM-UTDP-059/2024**

ASUNTO: RESPUESTA A LA SOLICITUD DE INFORMACIÓN RADICADA EN EL EXPEDIENTE TEEM-UT-SAIP-042/2024.

RECIBIDO
TRIBUNAL ELECTORAL DEL ESTADO
12 NOV 2024
UNIDAD DE TRANSPARENCIA

LIC. JUANA MARÍA LÓPEZ ZEPAHUA
JEFA DE DEPARTAMENTO "A" DE TRANSPARENCIA
DEL TRIBUNAL ELECTORAL DEL ESTADO
PRESENTE.

En atención al oficio **TEEM-TRANS-141/2024**, por medio del cual turna la solicitud de información con número de folio **160353224000046,** de fecha oficial de presentación veintiuno de octubre de dos mil veinticuatro, y mediante el cual, a su vez requiere a esta Oficialía de Datos Personales para que atienda diversos de los cuestionamientos, tengo a bien informar lo siguiente:

1. En relación con el cuestionamiento señalado con el numeral: ***"10. Informar si se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información Institucional por parte de los servidores públicos;".***

   Se informa que, como mecanismo de seguridad para mantener la confidencialidad de la información institucional, en el contrato de trabajo que celebra este órgano jurisdiccional con sus servidores públicos, se encuentra inserta una cláusula de confidencialidad en la que se prevé la obligación para que, durante la vigencia de la relación de trabajo y hasta un año posterior a su culminación, se mantenga en forma confidencial cualquier tipo de información con relación a las actividades del Tribunal.

   Esto con la finalidad de impedir la divulgación o utilización de dicha información para beneficio propio o de terceros, asimismo, en la misma cláusula se hace de conocimiento las posibles sanciones en caso de incumplimiento.

   Se pone a su disposición una versión del contrato en la siguiente liga: http://transparencia.teemcorreo.org.mx/sisofi_2018/uploads/11-10-2024/Contrato-Teemich.pdf

   Adicionalmente, se informa que en la Décima Primera Sesión Ordinaria del Comité de Transparencia se aprobó la implementación de la Recomendación 01/2024, relativa a la inserción de avisos de confidencialidad en las comunicaciones que se realizan mediante correos electrónicos.

Coronel Amado Camacho No. 294, Chapultepec Oriente, 58260 Morelia, Mich. • Tel. (443)1130130

2. Respecto al cuestionamiento número: "***11. Informar si la página web de la institución cuenta con: a) aviso de privacidad; b) certificados digitales vigentes;".***

   Con relación a lo cuestionado en el **inciso a),** se informa que en la página de internet del Tribunal Electoral del Estado (https://teemich.org.mx) se encuentran publicados los avisos de privacidad con que cuenta este órgano jurisdiccional. Mismos que se pueden consultar en el apartado de "TRANSPARENCIA", posteriormente, al abrirse el menú desplegable, en la opción "PROTECCIÓN DE DATOS PERSONALES", y finalmente en la sección denominada "AVISOS DE PRIVACIDAD INTEGRALES"; o bien, ingresando al siguiente enlace: https://teemich.org.mx/avisosdeprivacidadintegralysimplificado/.

   Por otra parte, se informa que actualmente se está trabajando en el proceso de actualización y generación de nuevos avisos de privacidad, por lo que cuando dicho proceso sea finalizado, los mismos serán publicados en la página institucional citada en el párrafo anterior.

   Ahora bien, respecto a lo consultado en el **inciso b),** informo que esta Oficialía de Datos Personales se ve imposibilitada para pronunciarse sobre la existencia de certificados digitales en la página de internet, toda vez que dicha temática escapa de las atribuciones, funciones y actividades que desempeña esta área. No obstante, se sugiere que dicho cuestionamiento sea remitido a la Unidad de Sistemas, al considerarse el área que conoce al respecto.

3. Por lo que ve a la información solicitada en el numeral: ***"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 de la organización participaron en su desarrollo e implementación?;".***

   Se informa que, sí existe un Sistema de Gestión relacionado con las medidas de seguridad para el tratamiento de datos personales. Para su desarrollo e implementación, participaron a través de la elaboración del inventario de datos personales, así como de los análisis de riesgos y de brecha, las siguientes áreas del Tribunal: Secretaría General de Acuerdos, Ponencia 1, Ponencia 2, Ponencia 3, Ponencia 5, Secretaría de Administración, Órgano Interno de Control, Coordinación de Capacitación, Investigación y Difusión del Derecho Electoral, Defensoría Jurídica, Coordinación de Archivo, Coordinación de Jurisprudencia y Estadística

Coronel Amado Camacho No. 294, Chapultepec Oriente, 58260 Morelia, Mich. • Tel. (443)1130130

Jurisdiccional, Coordinación de Género y Derechos Humanos, Coordinación de Comunicación Social y la Unidad de Transparencia.

Las actividades y acciones enfocadas en establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales se encuentran contenidas en el Documento de Seguridad que fue aprobado por el Comité de Transparencia del Tribunal Electoral del Estado el 21 de septiembre de 2023, mismo que se encuentra disponible para su consulta en https://teemich.org.mx/wp-content/uploads/2024/04/Documento-de-Seguridad.pdf.

4. En cuanto a la información solicitada en los números 17 y 35, relativa a: ***"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;"***, se otorgará una respuesta conjunta al tratarse del mismo cuestionamiento.

   En el Documento de Seguridad aprobado por el Comité de Transparencia del Tribunal Electoral del Estado el 21 de septiembre de 2023, se estableció el procedimiento para la notificación de la vulneración a la seguridad de los datos personales a su Titular, estipulando el plazo de 72 horas siguientes al registro de la vulneración para que el área tratante elabore el informe, mismo que se deberá notificar directamente al Titular a través de los medios que se establezca para tal fin, considerando la forma en que se obtuvieron los datos personales, el perfil de los titulares, la forma en que se mantiene contacto o comunicación con éstos, así como que sean gratuitos, de fácil acceso, con la mayor cobertura posible y que estén debidamente habilitados y disponibles en todo momento para el Titular.

   En dicho procedimiento participan las diversas áreas del Tribunal, dependiendo de cuál de ellas sea el área tratante de la información vulnerada: Secretaría General de Acuerdos, Ponencia 1, Ponencia 2, Ponencia 3, Ponencia 5, Secretaría de Administración, Órgano Interno de Control, Coordinación de Capacitación, Investigación y Difusión del Derecho Electoral, Defensoría Jurídica, Coordinación de Archivo, Coordinación de Jurisprudencia y Estadística Jurisdiccional, Coordinación de Género y Derechos Humanos, Coordinación de Comunicación Social y la Unidad de Transparencia.

5. En relación con lo cuestionado en los numerales 21 y 42, respecto a "**Informar si se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y cuáles son;"**, se otorgará una respuesta conjunta, al tratarse del mismo cuestionamiento.

Se informa que luego de una búsqueda exhaustiva en la información que obra en esta Oficialía de Datos, no se encontraron registros documentados de la adopción o implementación de esquemas de mejores prácticas en materia de protección de datos personales, precisando que conforme a lo dispuesto en el artículo 68 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo, la implementación de dichos esquemas es una posibilidad para el responsable, no así una obligación cuyo cumplimiento sea forzoso.

6. Respecto a la información solicitada en los numerales 22 y 43: ***"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 son han sido las recomendaciones vertidas por el INAI, en su caso;"***, se otorgará una respuesta conjunta, al tratarse del mismo cuestionamiento.

   Al respecto, se precisa que conforme al artículo 70 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo, es responsabilidad del responsable realizar una evaluación de impacto cuando se pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, o aplicaciones electrónicas que impliquen el tratamiento intensivo o relevante de datos personales. Por su parte, el artículo 71 de dicho ordenamiento, establece que se está ante un tratamiento intensivo o relevante cuando existan riesgos inherentes a los datos personales a tratar, cuando se traten datos personales sensibles, y cuando se efectúen o se pretendan efectuar transferencias de datos personales.

   De lo anterior, se desprende que las evaluaciones se deben realizar de forma previa a la implementación de los mecanismos que implican el tratamiento intensivo de datos personales; atento a ello, se informa que luego de una búsqueda exhaustiva en la información que obra en esta Oficialía de Datos Personales, no se encontró registro alguno de la realización de evaluaciones de impacto en materia de datos personales, de lo que se colige que este órgano jurisdiccional no se encuentra en el supuesto del uso de tecnologías que impliquen dichos tratamientos.

7. En cuanto al cuestionamiento identificado con el número: ***"23. Informar si se cuenta con documento de seguridad en materia de protección de datos personales;".***

Coronel Amado Camacho No. 294, Chapultepec Oriente, 58260 Morelia, Mich. • Tel. (443)1130130

Se informa que sí se cuenta con Documento de Seguridad, mismo que fue aprobado por el Comité de Transparencia del Tribunal Electoral del Estado el 21 de septiembre de 2023, mismo que se encuentra disponible para su consulta en https://teemich.org.mx/wp-content/uploads/2024/04/Documento-de-Seguridad.pdf.

8. Por lo que ve a la información solicitada en los numerales 26 y 45: ***"26. Informar si se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad;",*** se otorgará una respuesta conjunta, al tratarse del mismo cuestionamiento.

   Se informa que, si bien, hasta el momento no se han llevado a cabo auditorías internas o externas en materia de ciberseguridad, en el Plan de Trabajo se tiene contemplado elaborar un Programa de Auditoría Interna con apoyo del Instituto Michoacano de Transparencia, Acceso a la Información y Protección de Datos Personales, en virtud de que es el órgano especializado en la materia conforme a lo dispuesto en la Constitución del Estado, la Ley Estatal de Transparencia, la Ley Estatal de Datos y los Lineamientos Estatales de Datos; programa que en su momento, deberá ser aprobado por el Comité de Transparencia.

9. Con relación a lo cuestionado en numeral: ***"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?;".***

   Se informa que, de conformidad con lo establecido en el artículo 2 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, este Tribunal Electoral no es sujeto de la regulación de dicho ordenamiento.

Sin otro particular, remito la información solicitada, para los efectos correspondientes.

ATENTAMENTE

TRIBUNAL ELECTORAL DEL ESTADO
MICHOACÁN
OFICIALÍA DE DATOS
PERSONALES

LIC. JORGE TORRES REYES
OFICIAL DE DATOS PERSONALES ADSCRITO
A LA UNIDAD DE TRANSPARENCIA
DEL TRIBUNAL ELECTORAL DEL ESTADO

Coronel Amado Camacho No. 294, Chapultepec Oriente, 58260 Morelia, Mich. • Tel. (443)1130130


SIN TEXTO

SECRETARÍA DE ADMINISTRACIÓN
21 NOV. 2024
TRIBUNAL ELECTORAL DEL ESTADO DE MICHOACÁN
Hora 12:11 HRS.

Morelia, Michoacán a 21 de noviembre de 2024
Oficio: TEEM-TRANS-161/2024
Asunto: Se requiere información para atención de la Solicitud de Acceso a la Información con número de folio 160353224000046.

Mtro. Arturo Ángel Parra Luviano
Secretario de Administración;
M.E. Edgar Abdiel Barriga Delgado
Jefe de la Unidad de Sistemas;
ambos del Tribunal Electoral del Estado
Presente.

En seguimiento al diverso TEEM-TRANS-141/2024, de fecha veintitrés de octubre del año en curso, por medio del cual les fue remitido el ACUERDO DE INICIO Y TURNO dictado dentro del expediente TEEM-UT-SAIP-042/2024, a efecto de que las áreas a su cargo den respuesta a la Solicitud de Acceso a la Información 160353224000046; por medio del presente me permito solicitar su colaboración a efecto de que dicha información sea remitida a esta Unidad de Transparencia **a más tardar el día veintidós de noviembre de dos mil veinticuatro.**

Lo anterior, a efecto de poder estar en condiciones de cumplir con lo dispuesto por el artículo 75 de la Ley de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Michoacán, respecto a la fecha límite para dar respuesta a dicha solicitud, toda vez que la misma fue presentada por un particular el pasado veintiuno de octubre.

Sin más por el momento, me despido.

Atentamente

RNrAq8p937KXJP2wSoPlyYIwHsbX2j
LCDWB7y2M/2+o=
maria.lopez.zepahua@teemcorreo.org.mx

Lic. Juana María López Zepahua
Jefa de Departamento "A" de Transparencia
del Tribunal Electoral del Estado.

SISTEMAS INFORMÁTICOS
21 NOV. 2024
TRIBUNAL ELECTORAL DEL ESTADO DE MICHOACÁN
Hora: 12:15

TRIBUNAL ELECTORAL DEL ESTADO
UNIDAD DE TRANSPARENCIA

ACUSE

Este documento fue autorizado mediante firma electrónica certificada, y tiene plena validez jurídica de conformidad con el numeral TERCERO, CUARTO y QUINTO del ACUERDO DEL PLENO POR EL QUE SE IMPLEMENTA EL USO DE LA FIRMA ELECTRÓNICA EN LOS ACUERDOS, RESOLUCIONES Y SENTENCIAS QUE SE DICTEN CON MOTIVO DEL TRÁMITE, TURNO, SUSTANCIACIÓN Y RESOLUCIÓN DE LOS ASUNTOS JURISDICCIONALES, ASÍ COMO EN LOS ACUERDOS, LAS GESTIONES Y DETERMINACIONES DERIVADAS DEL ÁMBITO ADMINISTRATIVO DEL TRIBUNAL. ---


SIN TEXTO

TEEM-SA-224/2024
Morelia, Michoacán a 22 de noviembre de 2024

Lic. Juana María López Zepahua
Jefa Unidad de Transparencia
Tribunal Electoral del Estado
Presente

En atención al oficio TEEM-TRANS-141/2024, por el cual turna la solicitud de información con número de expediente TEEM-UT-SAIP-042/2024 y donde requiere que la Secretaría de Administración atienda lo referente a:

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;

b. informar si se cuenta con un 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.

18. Informar si se cuenta 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.

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

39. 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.

En respuesta a la solicitud, se informa lo siguiente:

La solicitud hace referencia a las Tecnologías de Información y Comunicación, razón por la cual, en la Secretaría de Administración no se tienen elementos para dar respuesta al total de cuestionamientos, no obstante, se proporciona la información correspondiente a las siguientes tres preguntas:

b. informar si se cuenta con un Inventario Institucional de bienes y servicios de TIC

Se adjunta enlace donde podrá consultar el inventario general de bienes del Tribunal, dentro del cual, se identifica el equipo informático.

http://transparencia.teemcorreo.org.mx/archexcel/disfinanciera/dis/2024/edof/Junio/INVENTARIO%20GENERAL%20TEEM%202024.pdf

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

Como parte del control y cuidado de los activos del Tribunal, los servidores públicos tienen resguardo de los bienes asignados, sin embargo, no se tiene un lineamiento en especifico referente al traslado de dispositivos móviles.

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 adjunta enlace donde podrá consultar la información curricular del Jefe de la Unidad de Sistemas del Tribunal.

http://transparencia.teemcorreo.org.mx/sisofi_2018/uploads/11-07-2023/Edgar-Abdiel-Barriga-Delgado.pdf

Sin otro particular, reciba un cordial saludo.

TRIBUNAL ELECTORAL DEL ESTADO DE MICHOACÁN SECRETARÍA DE ADMINISTRACIÓN

Atentamente

Mtro. Arturo Angel Parra Luviano
Secretario de Administración
Tribunal Electoral del Estado

C.c.p. Archivo.


SIN TEXTO

TEEMICH
TRIBUNAL ELECTORAL DEL ESTADO
MICHOACÁN

Morelia, Michoacán a 25 de noviembre de 2024
OFICIO: TEEM-SIS-038-2024

RECIBIDO
TRIBUNAL ELECTORAL DEL ESTADO
25 NOV 2024
12:11
UNIDAD DE TRANSPARENCIA

Lic. Juana María López Zepahua
Jefa de Departamento "A" de Transparencia
del Tribunal Electoral del Estado
Presente.

Por este medio, me permito informarle respecto a la información solicitada para el expediente interno TEEM-UT-SAIP-042/2024 respecto al apartado 1,2 y 3 en los puntos 1,2,y 3 no se cuenta con ningún tipo de información requerida a estos puntos para el punto 4 si se cuenta con una firma electrónica avanzada proporcionada por la empresa firmamex; para los puntos 5 y 6 no se cuenta con información al respecto para el punto 7 contamos con servicio de datos en la nube proporcionado por Google inc. para el punto 8 no se cuenta con lineamientos de seguridad. Para el punto 9 si se cuenta con correo electrónico así como con las características de los subapartados a,b,c,d y e; para los puntos 10,12,13,14,15,16,17,18,20,21,22,24,25,26,27,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,5 y 55 no se cuenta con los sistemas, mecanismos, lineamientos o información al respecto . Para el punto 11 si se cuenta con aviso de privacidad y certificados digitales vigentes.

Sin otro particular, reciba un cordial saludo.

A t e n t a m e n t e

M.E. Edgar Abdiel Barriga Delgado.
Jefe de Sistemas Informáticos.


SIN TEXTO