



**ACUERDO.- AYUNTAMIENTO CONSTITUCIONAL DE TUXTLA GUTIÉRREZ, CHIAPAS.-
COORDINACIÓN GENERAL DE LA UNIDAD DE TRANSPARENCIA.- TUXTLA GUTIÉRREZ,
CHIAPAS; A 15 DE NOVIEMBRE DEL 2024.**

Con fecha 30 de octubre del 2024, se tuvo por recibida a través de la Plataforma Nacional de Transparencia, la solicitud de acceso a la información pública con número de folio **070126124000285**, en la que se solicitó lo siguiente:

“Solicito la siguiente información 1. Informar sí dentro de la institución se cuenta con un gobierno de seguridad de la información o de ciberseguridad y cuáles áreas participan; 2. Señalar sí se han implementado las siguientes medidas: a) estándares técnicos definidos por la Coordinación de Estrategia Digital Nacional, en la contratación de bienes y servicios de seguridad de la información o de tecnologías de la información y comunicación; b) 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); 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). 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 sí en la contratación de servicios de seguridad de la información en Tecnologías de la Información y Comunicación y Seguridad de la Información, de ha contado con el Dictamen Técnico favorable expedido por la autoridad correspondiente; 7. Informar sí los servicios de centros de datos son propios, de otra institución gubernamental o de un tercero; 8. 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; 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. 9. Informar sí se cuentan con



mecanismos para evitar la divulgación no autorizada de datos o información Institucional por parte de los servidores públicos; 10. Informar si la página web de la institución cuenta con: a) aviso de privacidad; b) certificados digitales vigentes; 11. Informar si el personal responsable se ha capacitado en la implementación del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos; 12. 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; 13. 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 y cuántas horas de capacitación en ciberseguridad se realizan de forma anual. 14. 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?; 15. 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, lo anterior en términos de lo establecido por el artículos 40, 41 y 42 de la Ley general de protección de datos personales en posesión de sujetos obligados (LGPDPPSO); 16. 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, o anterior en términos de lo establecido por el artículos 40, 41 y 42 de la Ley general de protección de datos personales en posesión de sujetos obligados (LGPDPPSO);; 17. Informar si se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos; 18. 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. 19. Informar si han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas; 20. Informar si se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son; 21. 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; 22. Informas si se cuenta con documento de seguridad en materia de protección de datos personales; 23. Informar si se cuenta con un plan de comunicación institucional en caso de un incidente de ciberseguridad o seguridad de la información; 24. Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución; 25. Informar si se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad; 26. 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. Un help desk es un equipo centralizado dentro de una empresa que atiende incidencias y reportes de sistemas informáticos y software de una organización 27. Informar sí se cuenta con un Centro de Operaciones de Ciberseguridad Además informar si han tenido incidentes de ciberseguridad (sin importar ni decir cuáles)” (sic).

I.- Considerando que esta Coordinación General de la Unidad de Transparencia es competente para conocer y resolver las Solicitudes de Acceso a la Información Pública, con fundamento en lo dispuesto por los artículos 67, 69 y 70 fracción II de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas; le informo lo siguiente:

Su solicitud fue turnada a la Coordinación de Tecnologías de la Información y Comunicaciones de este Ayuntamiento. Dicha área, mediante oficio de respuesta de fecha 15 de noviembre del 2024, respectivamente, atendió conforme a sus atribuciones lo correspondiente, por lo que sírvase encontrar en forma anexa la información de mérito.

Por lo anterior expuesto y fundado, se tiene por contestada la solicitud en sentido de atención positiva a través de la presente resolución, información que conjuntamente deberá enviarse a través de la Plataforma Nacional de Transparencia Chiapas, para su notificación correspondiente.

ASÍ LO ACORDÓ, MANDA Y FIRMA EL COORDINADOR GENERAL DE LA UNIDAD DE TRANSPARENCIA, ING. GONZALO SOLIS LOPEZ, QUIEN ACTÚA CON FUNDAMENTO EN LOS ARTÍCULOS 67, 69, 70 fracción II y 158 DE LA LEY DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA DEL ESTADO DE CHIAPAS . - - - - -

- - - - -RÚBRICA. - - - - -



TUXTLA GUTIÉRREZ
AYUNTAMIENTO 2024-2027

COORDINACIÓN DE TECNOLOGÍAS DE LA
INFORMACIÓN Y COMUNICACIONES.

Tuxtla Gutiérrez, Chiapas a 15 de noviembre de 2024.

Oficio N° PM/CTIC/0226/2024.

Asunto: Respuesta a solicitud de acceso a la información.

Ing. Gonzalo Solís López.
Coordinador General de la Unidad de Transparencia.
Presente.

En atención a su Memorándum No. PM/CGUT/0038/2024 de fecha 31 de octubre de 2024, donde solicita responder a la solicitud de acceso a la información registrada con el número de folio 070126124000285; por lo anterior le envío las respuestas:

1. Si se cuenta, participan la Coordinación de Tecnologías de la Información y Comunicaciones a través de las áreas Depto. de Seguridad, Redes e Internet; Depto. de Normatividad e Infraestructura Tecnológica y el Depto. de Sistemas.
2.
 - a) No.
 - b) Si, a través de los dictámenes técnicos emitidos por el Depto. de Normatividad e Infraestructura Tecnológica; además se informa que se cuenta con un inventario institucional de bienes y servicios.
 - c) Si, implementado en junio de 2022.
 - d) Si, implementado en junio de 2022.
 - e) Si, a través de análisis de vulnerabilidades a las plataformas web (Ethical Hacking)
 - f) No
 - g) Si se cuenta, participan la Coordinación de Tecnologías de la Información y Comunicaciones a través de las áreas Depto. de Seguridad, Redes e Internet; Depto. de Normatividad e Infraestructura Tecnológica y el Depto. de Sistemas.
 - h) No.
 - i) Si se cuenta con un equipo de respuesta en la que intervienen la Coordinación de Tecnologías de la Información y Comunicaciones a través de las áreas Depto. de Seguridad, Redes e Internet; Depto. de Normatividad e Infraestructura Tecnológica y el Depto. de Sistemas.
3. No.
4. Si se cuenta con Firma Electrónica Avanzada.
5. Si se realizan simulacros.
6. Si se cuenta con dictamen técnico.
7. Se cuenta con centro de datos propio y también con terceros.
8. Si se cuenta con correo institucional.
 - a) No
 - c) Si
 - d) Si
 - e) Si
9. No.
10.
 - a) Si
 - b) Si

Sin más por el momento le envío un cordial saludo.

Atentamente

Mtra. Laura Margen Regalado Moreno.
Coordinadora.

c.c.p. Expediente.
Mtro LMRM/Dr SSA.

2ª Norte S/N, Col. Centro, Tuxtla Gutiérrez, Chiapas. C.P. 29000
Atención (961) 61 25511 | www.tuxtla.gob.mx



H. AYUNTAMIENTO CONSTITUCIONAL
DE TUXTLA GUTIÉRREZ
COORDINACIÓN GENERAL DE
LA UNIDAD DE TRANSPARENCIA

15 NOV 2024

HORA: 13:34 RECIBE:

RECIBIDO

SUJETO A REVISIÓN

¡Qué Viva!
Tuxtla!



TUXTLA GUTIÉRREZ
AYUNTAMIENTO 2024-2027

COORDINACIÓN DE TECNOLOGÍAS DE LA
INFORMACIÓN Y COMUNICACIONES.

Tuxtla Gutiérrez, Chiapas a 15 de noviembre de 2024.
Oficio N° PM/CTIC/0227/2024.
Asunto: Respuesta a solicitud de acceso a la información.

Ing. Gonzalo Solís López.
Coordinador General de la Unidad de Transparencia.
Presente.

En atención a su Memorándum No. PM/CGUT/0051/2024 de fecha 08 de noviembre de 2024, donde solicita responder a la solicitud de acceso a la información registrada con el número de folio 070126124000285; por lo anterior le envío las respuestas:

11. No.
12.
 - a) Si.
 - b) Si.
13. No.
14. No.
15. No.
16. No.
17. No.
18.
 - i) Si.
 - ii) Si.
 - iii) No.
 - iv) No.
19. No.
20. Si, Avisos de Privacidad y Documento de Seguridad.
21. Si se implica el tratamiento intensivo y/o relevante de datos personales (https://innovacion.tuxtla.gob.mx/taip/repositor/anexos_documentos/7b1506a8_08052023_1332.pdf). Pero no se han llevado evaluaciones de impacto por lo cual no hay recomendaciones del INAI.
22. Si. https://innovacion.tuxtla.gob.mx/taip/repositor/anexos_documentos/7b1506a8_08052023_1332.pdf.
23. No.
24. Si cada 12 meses.
25. Si cada 12 meses.
26. Si, auditoría de seguridad externa.
27. Si se cuenta con Centro de Operaciones de Ciberseguridad, si se han tenido incidentes de ciberseguridad.

Sin más por el momento le envío un cordial saludo.



H. AYUNTAMIENTO CONSTITUCIONAL
DE TUXTLA GUTIÉRREZ
COORDINACIÓN GENERAL DE
LA UNIDAD DE TRANSPARENCIA

15 NOV 2024

HORA: 13:34 RECIBE:

RECIBIDO
SUJETO A REVISIÓN

Atentamente

Mtra. Laura Murgeny Regalado Moreno.
Coordinadora.



2ª Norte S/N, Col. Centro, Tuxtla Gutiérrez, Chiapas. C.P. 29000
Atención (961) 61 25511 | www.tuxtla.gob.mx

¡Qué viva
Tuxtla!



MEMORÁNDUM No. PM/CGUT/0051/2024
TUXTLA GUTIÉRREZ, CHIAPAS A 08 DE NOVIEMBRE DEL 2024

MTRA. LAURA MARGENY REGALADO MORENO
COORDINADORA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES
P R E S E N T E

Por este medio, y en alcance al Memorándum No. PM/CGUT/0038/2024, a través del cual se requirió la atención de la solicitud de acceso a la información pública con número de folio 070126124000285, me permito remitir los siguientes planteamientos, realizados por la misma persona solicitante:

11. Informar si el personal responsable se ha capacitado en la implementación del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos;
12. 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;
13. 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 y cuántas horas de capacitación en ciberseguridad se realizan de forma anual.
14. 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?;
15. 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, lo anterior en términos de lo establecido por el artículos 40, 41 y 42 de la Ley general de protección de datos personales en posesión de sujetos obligados (LGPDPPO);
16. 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, o anterior en términos de lo establecido por el artículos 40, 41 y 42 de la Ley general de protección de datos personales en posesión de sujetos obligados (LGPDPPO);;
17. Informar si se cuentan con lineamientos para el traslado de activos físicos (dispositivos móviles) de la institución, por parte de los servidores públicos;
18. 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.



TUXTLA GUTIÉRREZ
AYUNTAMIENTO 2024-2027

COORDINACIÓN GENERAL DE LA UNIDAD DE
TRANSPARENCIA

19. Informar si han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas;
20. Informar si se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son;
21. 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;
22. Informar si se cuenta con documento de seguridad en materia de protección de datos personales;
23. Informar si se cuenta con un plan de comunicación institucional en caso de un incidente de ciberseguridad o seguridad de la información;
24. Informar cada cuanto tiempo se actualizan las medidas de ciberseguridad dentro de la institución;
25. Informar si se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad;
26. 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. Un help desk es un equipo centralizado dentro de una empresa que atiende incidencias y reportes de sistemas informáticos y software de una organización
27. Informar si se cuenta con un Centro de Operaciones de Ciberseguridad Además informar si han tenido incidentes de ciberseguridad (sin importar ni decir cuáles)

Para la atención integral de lo anterior, me permito proporcionar como término para el cumplimiento de este y el Memorándum No. PM/CGUT/0038/2024 el día 20 de noviembre del año en curso, con la finalidad de proporcionar en tiempo y forma la información requerida ante la Plataforma Nacional de Transparencia, o en su defecto, los motivos por los que esta solicitud no pueda ser atendida.

Sin otro en particular, aprovecho la ocasión para enviarle un cordial saludo.

Atentamente

Ing. Gonzalo Solís López
Coordinador General de la Unidad de Transparencia



H. AYUNTAMIENTO CONSTITUCIONAL
DE TUXTLA GUTIÉRREZ
COORDINACIÓN GENERAL DE
LA UNIDAD DE TRANSPARENCIA

08 NOV 2024

HORA:

DESPACHADO



MEMORÁNDUM No. PM/CGUT/0038/2024
TUXTLA GUTIÉRREZ, CHIAPAS A 31 DE OCTUBRE DEL 2024

MTRA. LAURA MARGENY REGALADO MORENO
COORDINADORA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

P R E S E N T E

Por este medio, con fundamento en lo establecido por los artículos 67, 69 y 70 fracciones II y IV, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas, y derivado de la solicitud de acceso a la información pública registrada con el número de folio 070126124000285, me permito solicitar de usted que a más tardar el día 15 de noviembre del año en curso, se sirva informar, de acuerdo a las funciones y atribuciones de esa coordinación, lo siguiente:

"Solicito la siguiente información:

- 1. Informar si dentro de la institución se cuenta con un gobierno de seguridad de la información o de ciberseguridad y cuáles áreas participan;**
- 2. Señalar si se han implementado las siguientes medidas: a) estándares técnicos definidos por la Coordinación de Estrategia Digital Nacional, en la contratación de bienes y servicios de seguridad de la información o de tecnologías de la información y comunicación; b) mejores prácticas aplicables a la gestión de las TIC en los diferentes procesos de contratación para la adquisición, el arrendamiento de bienes o la prestación de servicios en materia de TIC y de seguridad de la información; Informar si se cuenta con 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); 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).**
- 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 en la contratación de servicios de seguridad de la información en Tecnologías de la Información y Comunicación y Seguridad de la Información, de ha contado con el Dictamen Técnico favorable expedido por la autoridad correspondiente;**





7. Informar si los servicios de centros de datos son propios, de otra institución gubernamental o de un tercero;
8. 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; 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.
9. Informar si se cuentan con mecanismos para evitar la divulgación no autorizada de datos o información Institucional por parte de los servidores públicos;
10. Informar si la página web de la institución cuenta con: a) aviso de privacidad; b) certificados digitales vigentes;" (SIC)

Lo anterior con la finalidad de proporcionar en tiempo y forma la información requerida ante la Plataforma Nacional de Transparencia, o en su defecto, los motivos por los que esta solicitud no pueda ser atendida.

Sin otro en particular, aprovecho la ocasión para enviarle un cordial saludo.

Atentamente

Ing. Gonzalo Solís López

Coordinador General de la Unidad de Transparencia



DESPOCHADO