ÁREA: Unidad de Transparencia Municipal

OFICIO NÚM. UT/1432/2024

ASUNTO: Respuesta a solicitud de acceso a la información pública con número de folio 201172324000290

Oaxaca de Juárez, Oaxaca, 14 de noviembre de 2024.

SOLICITANTE.
P R E S E N T E.

En respuesta a su solicitud de acceso a la información pública con número de folio 201172324000290 presentada a través de la Plataforma Nacional de Transparencia el 30 de octubre último, requiriendo textualmente 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 sí la página web de la institución cuenta con: a) aviso de privacidad; b) certificados digitales vigentes; Otros datos para su localización
11. Informar sí 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 seguirdad de la información; b) Indicadores que permitan medir la 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 si se cuenta con un Centro de Operaciones de Ciberseguridad Además informar si han tenido incidentes de ciberseguridad (sin importar ni decir cuáles.

Por lo anterior, con fundamento en lo establecido en los artículos 6º apartado A, fracción I de la Constitución Política de los Estados Unidos Mexicanos; 3º y 114 apartado C de la Constitución Política del Estado Libre y Soberano de Oaxaca; 6º, 42, 44 fracción II y 136 de la Ley General de Transparencia y Acceso a la Información Pública, y 1º. 6º fracción XLI y 68 de la Ley de Transparencia, Acceso a la Información y Buen Gobierno para el Estado de Oaxaca, se atiende en los siguientes términos:

Mediante similar número DSI/1411-1/2024 el Ing. Alfonso Sandoval Carballido, director de Sistemas de la Información del Municipio de Oaxaca de Juárez, da respuesta a su requerimiento de información, en los términos del oficio de referencia.

Unidad de Transparencia

En el supuesto de no estar conforme con la respuesta otorgada, se hace de su conocimiento que conforme a los artículos 133, 137, 138 y 139 de la Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno del Estado de Oaxaca, tiene el derecho a interponer un recurso de revisión dentro de los quince días hábiles siguientes a la fecha en que surta efectos la presente notificación.

Finalmente, considerando que el ejercicio del derecho de acceso a la información pública contribuye al fortalecimiento de espacios de participación que fomentan la interacción entre la sociedad y los sujetos obligados, me permito reiterarle que esta Unidad de Transparencia, queda a sus órdenes.

Sin más por el momento, quedo a sus ordenes.

A T E N T A M E N T E
"EL RESPETO AL DERECHO AJENO ES LA PAZ"
"POR UNA CIUDAD EDUCADORA"

LICDA. KEYLA MATUS MELÉNDEZ.
TITULAR DE LA UNIDAD DE TRANSPARENCIA MUNICIPAL.

UNIDAD DE
TRANSPARENCIA

C.c.p.- Expediente.
KMM´ert

Oaxaca de Juárez
CIUDAD EDUCADORA

MUNICIPIO DE
OAXACA DE JUÁREZ, OAX.
2022 - 2024

Oaxaca de Juárez
2022 - 2024

OAXACA

Ciudades Mexicanas
PATRIMONIO MUNDIAL

RECIBIDO
12 46 hrs
14 NOV 2024

UNIDAD DE TRANSPARENCIA

"2024, Bicentenario de la Integración de Oaxaca a la República Mexicana".

OFICIO: DSI/1411-1/2024
ASUNTO: Respuesta a Solicitud de Información.

Oaxaca de Juárez, Oaxaca, 14 de noviembre de 2024

LIC. KEYLA MATUS MELÉNDEZ
JEFA DE LA UNIDAD DE TRANSPARENCIA
P R E S E N T E:

En respuesta a su oficio UT/1364/2024 en el cuál solicita información derivada de la solicitud de acceso a la Información Pública con número de folio 201173224000290, recibida a través de la Plataforma Nacional de Transparencia

Se remite la siguiente respuesta a su solicitud de información:

1.- Informar sí dentro de la institución se cuenta con un gobierno de seguridad de la información o de ciberseguridad y cuales áreas participan.

RESPUESTA: INFORMACIÓN CLASIFICADA COMO RESERVADA.

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;

RESPUESTA: NO

b) mejores prácticas aplicables a la gestión de las TIC en los diferentes procesos de contratación para la adquisición, e/ 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;

Respuesta: NO

c) un plan de continuidad de operaciones, y señalar la fecha de implementación;

RESPUESTA: INFORMACIÓN CLASIFICADA COMO RESERVADA.

d) Informar si se ha desarrollado e implementado el plan de recuperación ante desastres, señalar la fecha de desarrollo e implementación;

RESPUESTA: INFORMACIÓN CLASIFICADA COMO RESERVADA.

Dirección de
Sistemas de Información

e) desarrollado e implementado un programa de gestión de vulnerabilidades.

RESPUESTA: INFORMACIÓN CLASIFICADA COMO RESERVADA.

f) Marco de Gestión de Seguridad de la Información MGSI),

RESPUESTA: INFORMACIÓN CLASIFICADA COMO RESERVADA.

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;

RESPUESTA: INFORMACIÓN CLASIFICADA COMO RESERVADA.

h) informar si se cuenta con un diagnóstico de identificación de los procesos y activos esenciales de la Institución

RESPUESTA: NO

i) informar sse cuenta con un Equipo de Respuesta a incidentes de segundad de la Información (ERISC).

RESPUESTA: INFORMACIÓN CLASIFICADA COMO RESERVADA.

3.- Informar si es que se cuenta con una estrategia de ciber seguridad 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 sí se implementado la firma electrónica avanzada en la institución.

RESPUESTA: NO.

5.- informar si se realizan Simulacros sobre el plan de recuperación de desastres o en caso de incidentes cibernéticos.

RESPUESTA: INFORMACIÓN CLASIFICADA COMO RESERVADA.

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, se ha contado con el dictamen Técnico favorable expedido por la autoridad correspondiente.

RESPUESTA: SI.

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

RESPUESTA: INFORMACIÓN CLASIFICADA COMO RESERVADA.

Dirección de
Sistemas de Información

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;

RESPUESTA: SI

c) control institucional de la totalidad de los correos contenidos en las carpetas de los usuarios;

RESPUESTA: INFORMACIÓN CLASIFICADA COMO RESERVADA.

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;

RESPUESTA: INFORMACIÓN CLASIFICADA COMO RESERVADA.

e) cuenta con cifrado en el envío de información.

RESPUESTA: INFORMACIÓN CLASIFICADA COMO RESERVADA.

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

RESPUESTA: INFORMACIÓN CLASIFICADA COMO RESERVADA.

10.- Informar si la página web de la institución cuenta con:

a) aviso de privacidad;

RESPUESTA: SI

b) certificados digitales vigentes.

RESPUESTA: SI

11.- Informar si el personal responsable se ha capacitado en la implementación del Protocolo Nacional Homologado para la Gestión de incidentes Cibernéticos.

RESPUESTA: INFORMACIÓN CLASIFICADA COMO RESERVADA.

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;

RESPUESTA: INFORMACIÓN CLASIFICADA COMO RESERVADA.

b) indicadores que permitan medir la madurez institucional en la gestión de seguridad de la información.

RESPUESTA: INFORMACIÓN CLASIFICADA COMO RESERVADA.

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 cuando se implementó y cuántas horas de capacitación en ciberseguridad serealizan de forma anual.

RESPUESTA: INFORMACIÓN CLASIFICADA COMO RESERVADA.

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

RESPUESTA. NO

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 le la institución que participan?' e informar desde cuándo se implementó, lo anterior en términos de lo establecido por los artículos 40, 41 y 42 de la Ley general de protección de datos personales en posesión de sujetos obligados LGPDPPSO).

RESPUESTA: NO.

16. 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, o anterior en términos de lo establecido por el artículo 40, 41 y 42 de la Ley general de protección de datos personales en posesión de sujetos obligados (LGPDPPSO).

RESPUESTA NO

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 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.

RESPUESTA: INFORMACIÓN CLASIFICADA COMO RESERVADA.

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

RESPUESTA: INFORMACIÓN CLASIFICADA COMO RESERVADA.

20.- Informar si se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuales son.

RESPUESTA: NO.

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 cuales han sido las recomendaciones vertidas por el del INAI, en su caso.

RESPUESTA: INFORMACIÓN CLASIFICADA COMO RESERVADA.

22.- Informar si se cuenta con incremento de seguridad en materia de protección de datos personales.

RESPUESTA: INFORMACIÓN CLASIFICADA COMO RESERVADA.

23.- Informar si se cuenta con un plan de comunicación institucional en caso de un incidente de ciberseguridad o seguridad de la información.

RESPUESTA: NO

24.- Informar cada cuanto tiempo se actualizan las medidas de seguridad dentro de la institución.

RESPUESTA: INFORMACIÓN CLASIFICADA COMO RESERVADA

25.- Informar sí se llevan auditorias de seguridad externas. y/o internas en materia de ciberseguridad, así como su periodicidad.

RESPUESTA: INFORMACIÓN CLASIFICADA COMO RESERVADA.

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 externó. Un help desk es un equipo centralizado dentro de una empresa que atiende incidencias y reportes de sistemas informáticos y software de una organización.

RESPUESTA: NO

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).

RESPUESTA: INFORMACIÓN CLASIFICADA COMO RESERVADA.

Como ya se estableció en líneas anteriores, respecto de las preguntas marcadas como: 1, 2 (incisos c, d, e f , g , i) , 3 , 4 , 5 , 7 ,8 (incisos c , d , e), 9,11, 12. 13, 14, 17, 18 , 19, 21, 22, 24 ,25 , 27.La información solicitada encuadra como información reservada en términos de lo dispuesto en los artículos 110, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública y 100, 113, fracción I de la Ley General de Transparencia y Acceso a la Información Pública. 54 fracción II de la Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno del Estado de Oaxaca y los numerales Octavo, párrafo tercero y Trigésimo Cuarto de los Lineamientos en materia de Clasificación y Desclasificación de la Información, así como para la elaboración de versiones públicas,, Lo anterior con base en lo siguiente:

Con fundamento en el artículo 104 de la Ley General de Transparencia y Acceso a la Información Pública, de hacer entrega de la información a que se refiere la solicitud de acceso a la información que nos ocupa, existe un riesgo real, demostrable e identificable de perjuicio significativo al interés público, toda vez que con la difusión de la información relacionada a Mecanismos, estrategias y herramientas de ciberseguridad implementadas, ubicación de la información y procesos de recuperación de desastres y continuidad de operaciones, implicaría colocar en un estado de vulnerabilidad al Municipio de Oaxaca de Juárez, ya que se comprometería la seguridad informática de los sistemas y porque se pondría en riesgo la seguridad operativa de la infraestructura tecnológica que permite la operación de las diversas áreas que conforman el H. Ayuntamiento de Oaxaca de Juárez, superándose el interés público general de que al difundirse la información, se compromete y menoscaba la seguridad pública municipal y la certeza de los ciudadanos que acuden al H. Ayuntamiento a realizar diversos trámites poniendo en un estado total de vulnerabilidad tanto a las personas como a la institución, facilitando la intervención de las comunicaciones y permitiendo usurpar permisos requeridos en la red para obtener información; así también se darían a conocer puntos de vulnerabilidad para la seguridad de la infraestructura de cómputo, así como de la ubicación del centro de datos; Vulneraría sus sistemas informáticos e información contenida en éstos; además de que atentaría contra de su infraestructura tecnológica, afectando el ejercicio de sus labores sustantivas; que podría ocasionar la modificación, destrucción y pérdida de la información contenida en los sistemas.

En tal virtud, Clasificar la información como reservada se adecua al principio de proporcionalidad, en tanto que se justifica negar su divulgación, aunado a que, la clasificación constituye el medio menos lesivo para la adecuada protección del bien jurídico tutelado, como es la seguridad pública municipal, con base en lo que dispone el artículo 6° apartado A de la Constitución Política de los Estados Unidos Mexicanos, que, la información que tienen bajo su resguardo los sujetos obligados del Estado encuentra como excepción aquella que sea temporalmente reservada o confidencial en los términos establecidos, y cuando de su difusión pueda derivarse un perjuicio a la seguridad pública municipal o al interés público, como acontece en el presente caso.

Por lo anterior, no es posible entregar la información solicitada.

Sin más por el momento le envío un cordial saludo.

ATENTAMENTE
"EL RESPETO AL DERECHO AJENO ES LA PAZ"
"POR UNA CIUDAD EDUCADORA"

ING. ALFONSO SANDOVAL CARBALLIDO
DIRECTOR DE SISTEMAS DE INFORMACIÓN

DIRECCIÓN DE SISTEMAS DE INFORMACIÓN