



TRIBUNAL DE ARBITRAJE
Y ESCALAFÓN

GOBIERNO DEL ESTADO

UNIDAD DE TRANSPARENCIA

EXPEDIENTE. 184/2024-T

En la ciudad de Guadalajara, Jalisco, siendo las 12:00 doce horas del día 06
seis de noviembre del año 2024 dos mil veinticuatro. - - - - -

VISTAS y analizadas la totalidad de las actuaciones que integran el presente
procedimiento de acceso a la información pública, de conformidad a lo dispuesto
por los artículos 24 punto 1 fracción II, 77 punto 1 fracción II, 83, 84, 85 y 86 de la
Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus
Municipios, la Unidad de Transparencia del Tribunal de Arbitraje y Escalafón del
Estado de Jalisco, tiene a bien el resolver el Expediente **184/2024-T**, relativo a la
solicitud de acceso a la información presentada vía Plataforma Nacional en esta
Unidad de Transparencia, a la que se le asignó el número de folio
141233024000127, en la que se solicitó 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 de conformidad con el Acuerdo por el que se emiten políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y la comunicación, y la seguridad de la información en la Administración Pública Federal, publicado en el DOF el 6 de septiembre de 2021, 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 una Inventario Institucional de bienes y servicios de TIC; c) un plan de continuidad de operaciones, y señalar la fecha de implementación; d) Informar si se ha desarrollado e implementado el plan de recuperación ante desastres, señalar la fecha de desarrollo e implementación; e) desarrollado e implementado un programa de gestión de vulnerabilidades; f) Marco de Gestión de Seguridad de la Información (MGSI); 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 CEDN, de conformidad con el Acuerdo por el que se emiten políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y la comunicación, y la seguridad de la información en la Administración Pública Federal, publicado en el DOF el 6 de septiembre de 2021 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;

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



UNIDAD DE TRANSPARENCIA

EXPEDIENTE. 184/2024-T

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. 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 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, la Titular de la Unidad de Transparencia del Tribunal de Arbitraje y Escalafón del Estado de Jalisco, procede a: - - - - -

R E S O L V E R

PRIMERO.- Que del análisis practicado al contenido de la referida solicitud de acceso a la información pública, esta Unidad de Transparencia tuvo a bien ordenar con fundamento en lo dispuesto por los artículos 5°, 25 punto 1 fracción VII, 31 y 32 punto 1 fracciones III y VIII de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, se proceda a realizar la búsqueda de la información solicitada, en el área que conforme a sus obligaciones y atribuciones se estimó es competente o que pudiese tenerla, por lo que al reunir los requisitos de ley y actualizarse la hipótesis establecida en los artículos 79, 82 punto 1 y 83 puntos 1 y 2 de la misma Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, esta Unidad de Transparencia tuvo a bien registrarla internamente en el índice de este sujeto obligado, integrando y desahogando el procedimiento administrativo correspondiente, por lo que una vez realizada la búsqueda de la información requerida en las áreas competentes, siendo esto con el **ENCARGADO Del ÁREA DE INFORMÁTICA Y ESTADISTICA**, así como a la **TITULAR DEL ÁREA ADMINISTRATIVA** de este Tribunal, quienes tuvieron a bien remitir a esta Unidad de Transparencia la repuesta a la información peticionada de la siguiente forma: - - - - -

El área administrativa dijo: - - - - -

"Por este conducto doy contestación a su oficio UT/364/2024 de fecha 31 treinta y uno de octubre del año en curso, en el que se solicitan diversos cuestionamientos relativos a la ciberseguridad y protección de datos en esta dependencia, informándole que, de la totalidad de lo solicitado, únicamente corresponde a esta área emitir contestación al punto marcado como 18, por lo que se manifiesta lo siguiente:



TRIBUNAL DE ARBITRAJE
Y ESCALAFÓN

GOBIERNO DEL ESTADO

UNIDAD DE TRANSPARENCIA

EXPEDIENTE. 184/2024-T

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.

Respuesta: del expediente laboral de las personas encargadas de sistemas de información y su correspondiente curriculum, no se desprende que cuenten con conocimientos comprobables en las materias que señala.."

El encargado del área de Informática y Estadística manifestó: - - - - -

"2. Señalar si de conformidad con el Acuerdo por el que se emiten políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y la comunicación, y la seguridad de la información en la Administración Pública Federal, publicado en el DOF el 6 de septiembre de 2021, 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;

NO

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;

Si

Informar si se cuenta con una Inventario Institucional de bienes y servicios de TIC;

Si

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

SI SE CUENTA CON UN PLAN, SIN EMBARGO, AUN NO SE CUENTA CON FECHA DE IMPLEMENTACIÓN

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

SI SE CUENTA CON UN PLAN, SIN EMBARGO, AUN NO SE CUENTA CON FECHA DE IMPLEMENTACIÓN

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

SI

f) Marco de Gestión de Seguridad de la Información (MGSI);

SI

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;

Si, el área de informática



UNIDAD DE TRANSPARENCIA

EXPEDIENTE. 184/2024-T

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

si

i) Informar si se cuenta con un Equipo de Respuesta a Incidentes de Seguridad de la Información (ERISC).

Si

3. Informar si es que se cuenta con una estrategia de ciberseguridad dentro de la institución, en caso de respuesta afirmativa, informar lo siguiente

Si

(i) referir la fecha de creación;

año 2023

(ii) la fecha de implementación,

año 2024

(iii) si es que se ha actualizado o modificado y en cuántas ocasiones;

solo en el año 2024

(iv) cuáles áreas participaron en la creación de dicha estrategia ;

informática

4. Informar si se emplea la firma electrónica avanzada en la institución;

No

5. Informar si se realizan simulacros sobre el plan de recuperación de desastres o en caso de incidentes cibernéticos;

Si

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 CEDN, de conformidad con el Acuerdo por el que se emiten políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y la comunicación, y la seguridad de la información en la Administración Pública Federal, publicado en el DOF el 6 de septiembre de 2021

NO

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

Propios

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:

Si

a) inserción de leyenda de confidencialidad de la información;



**TRIBUNAL DE ARBITRAJE
Y ESCALAFÓN**

GOBIERNO DEL ESTADO

UNIDAD DE TRANSPARENCIA

EXPEDIENTE. 184/2024-T

si

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

si

c) 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;

Si

d) cuenta con cifrado en el envío de información.

si

11. Informar sí el personal responsable se ha capacitado en la implementación del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos;

No

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;

si

b) Indicadores que permitan medir el madurez institucional en la gestión de seguridad de la información;

no

13. 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 y cuántas horas de capacitación en ciberseguridad se realizan de forma anual.

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;

No

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

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 cuáles han sido las recomendaciones vertidas por el del INAI, en su caso;

No



UNIDAD DE TRANSPARENCIA

EXPEDIENTE. 184/2024-T

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

Si

24. Informar cada cuanto tiempo de actualizan las medidas de ciberseguridad dentro de la institución;

Aproximadamente cada tres meses

25. Informar si se llevan auditorías de seguridad externas y/o internas en materia de ciberseguridad, así como su periodicidad;

No

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

Si

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)

Si"

Por otro lado, en cuanto a los cuestionamientos marcados con los números 1, 9, 10, 14, 15, 16, 20 y 22, es preciso señalar que esta Unidad es competente para dar contestación a las mismas, lo que se realiza en este acto de la siguiente forma:

"1. Informar si dentro de la institución se cuenta con un gobierno de seguridad de la información o de ciberseguridad y cuáles áreas participan;

RESPUESTA: No se cuenta con un gobierno de seguridad de la información en esta dependencia

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

RESPUESTA: Si, los establecidos en el aviso de privacidad integral de la dependencia:

<https://transparenciasitgej.jalisco.gob.mx/api/api/archivos/1397/download?inline=true>

10. Informar si la página web de la institución cuenta con: a) aviso de privacidad; b) certificados digitales vigentes;

RESPUESTA: Si se cuenta

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: El sistema de gestión de datos se encuentra dentro del documento de seguridad de este Sujeto Obligado, mismo que fue elaborado conforme a la Ley vigente, el desarrollo fue a cargo de la unidad de transparencia.

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



TRIBUNAL DE ARBITRAJE
Y ESCALAFÓN

GOBIERNO DEL ESTADO

UNIDAD DE TRANSPARENCIA

EXPEDIENTE. 184/2024-T

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);

No se cuenta con un modelo sistema específico

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);;

No se cuenta con un modelo sistema específico

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

Solo los establecidos en la Ley

22. Informas si se cuenta con documento de seguridad en materia de protección de datos personales;

Si"

SEGUNDO.- Se tiene a las áreas correspondientes informando lo relacionado a los puntos de la solicitud información, en cuanto al ejercicio de sus funciones. Por lo antes descrito y de conformidad a lo establecido por los artículos 24 punto 1 fracción II, 77, 83, 84, 85, y 86 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; esta Unidad de Transparencia del Tribunal de Arbitraje y Escalafón del Estado de Jalisco, resuelve en sentido **AFIRMATIVO**, a su solicitud de información, por los motivos expuestos con anterioridad. - - - - -

NOTIFÍQUESE AL SOLICITANTE VÍA PLATAFORMA NACIONAL DE TRANSPARENCIA.- - - - - -

Así lo acordó la Licenciada Karla Georgina Martín Acosta Titular de la Unidad de Transparencia de este Tribunal de Arbitraje y Escalafón del Estado de Jalisco.-

