Av. Santa Fe # 27
Col. Yerbabuena | C.P. 36250
Guanajuato, Gto.

TRIBUNAL ESTATAL ELECTORAL
DE GUANAJUATO

473 732 9597 | 473 732 8091
473 732 2839
www.teegto.org.mx

Oficio No: TEEG-UT-287/2024
Guanajuato, Gto., 06 de noviembre de 2024
Asunto: Respuesta a solicitud
de acceso a la información

C. Solicitante de acceso a la información
P R E S E N T E.-

En atención a la solicitud de **ACCESO A LA INFORMACIÓN PÚBLICA** presentadas a través de la Plataforma Nacional de Transparencia, con fecha **30 de octubre del 2024**, identificada con el folio **110200200012224**; con fundamento en los artículos 6°, inciso A de la *Constituc0ión Política de los Estados Unidos Mexicanos*; 14, inciso B de la *Constitución Política para el Estado de Guanajuato*; 1°, 2°, 3°, 4°, 19, 47 y 48, fracciones II, III, IV y V, 82, 83, 85, 99 y demás aplicables de la *Ley de Transparencia y Acceso a la Información Pública para el Estado de Guanajuato*; 57 y 58 inciso a) del *Reglamento Interior del Tribunal Estatal Electoral*; así como los artículos 5, 6, 7, 10, 12, fracciones I, VII y VIII, 15, fracciones I, II y X, 38, 40, 44, 45, 46, 47, 48, 49, 52, 53, 54, 74, 75 y 76 del *Reglamento de Transparencia, Acceso a la Información y Protección de Datos Personales del Tribunal Estatal Electoral de Guanajuato*; esta Unidad de Transparencia, es competente para recibir, tramitar, orientar, requerir, prevenir y **dar respuesta** de la siguiente información:

> *"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 sí la página web de la institución cuenta con: a) aviso de privacidad; b) certificados digitales vigentes; 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 el madurez institucional en la*

gestión de seguridad de la información; 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. 14. 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?; 15. 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, 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 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 artículos 40, 41 y 42 de la Ley general de protección de datos personales en posesión de sujetos obligados (LGPDPPSO);; 17. Informar sí 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. 19. Informar sí han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas; 20. Informar sí se han adoptado esquemas de mejores prácticas en materia de protección de datos personales y señalar cuáles son; 21. 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; 22. Informas sí se cuenta con documento de seguridad en materia de protección de datos personales; 23. Informar sí 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 sí 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)

Por este conducto y en respuesta a su solicitud de acceso a la información, el **Órgano Interno de Control**, mediante oficio **TEEG-OIC-292/2024**, de fecha **04 de noviembre de 2024**, precisa lo siguiente:

Por medio del presente y en relación al oficio número **TEEG-UT-279/2024** de fecha 30 de octubre de 2024, a través del cual remite la solicitud de acceso a la información identificada con el folio número **110200200012224,** recibida vía Plataforma Nacional de Transparencia el 30 de octubre del año en curso; proporciono la respuesta en los términos siguientes:

Del oficio en mención, se advierte que se encuentra dirigido a dos áreas integrantes de este Tribunal en función del ámbito de competencia que a cada una le corresponde, siendo a este Órgano Interno de Control lo relativo a la pregunta identificada con el número 25.

En ese sentido, el solicitante refiere:

Solicito la siguiente información

(…)

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

(…)

Previo a entrar al análisis del punto antes referido, es de precisar que el solicitante no señala claramente la temporalidad respecto de la cual solicita la información, por lo que en lo conducente se estará a lo establecido en el criterio de interpretación para sujetos obligados reiterado y vigente número SO/003/2019, que se transcribe a continuación:

> ***Periodo de búsqueda de la información.*** *En el supuesto de que el particular no haya señalado el periodo respecto del cual requiere la información, o bien, de la solicitud presentada no se adviertan elementos que permitan identificarlo, deberá considerarse, para efectos de la búsqueda de la información, que el requerimiento se refiere al año inmediato anterior, contado a partir de la fecha en que se presentó la solicitud.*

En relación al punto identificado como **25**, se **informa** al solicitante que a la fecha en que se atiende su petición, no se han llevado a cabo auditorías de seguridad tanto externas como internas en materia de ciberseguridad por lo que la información solicitada es inexistente. Ello de conformidad con los criterios del Instituto Nacional de Acceso a la Información números 07/17 y 03/17, mismos que a continuación se transcriben:

Casos en los que no es necesario que el Comité de Transparencia confirme formalmente la inexistencia de la información. La Ley General de Transparencia y Acceso a la Información Pública y la Ley Federal de Transparencia y Acceso a la Información Pública establecen el procedimiento que deben seguir los sujetos obligados cuando la información solicitada no se encuentre en sus archivos; el cual implica, entre otras cosas, que el Comité de Transparencia confirme la inexistencia manifestada por las áreas competentes que hubiesen realizado la búsqueda de la información. No obstante, lo anterior, en aquellos casos en que no se advierta obligación alguna de los sujetos obligados para contar con la información, derivado del análisis a la normativa aplicable a la materia de la solicitud; y además no se tengan elementos de convicción que permitan suponer que ésta debe obrar en sus archivos, no será necesario que el Comité de Transparencia emita una resolución que confirme la inexistencia de la información.

> ***No existe obligación de elaborar documentos ad hoc para atender las solicitudes de acceso a la información.*** *Los artículos 129 de la Ley General de Transparencia y Acceso a la Información Pública y 130, párrafo cuarto, de la Ley Federal de Transparencia y Acceso a la Información Pública, señalan que los sujetos obligados deberán otorgar acceso a los documentos que se encuentren en sus archivos o que estén obligados a documentar, de acuerdo con sus facultades, competencias o funciones, conforme a las características físicas de la información o del lugar donde se encuentre. Por lo anterior, los sujetos obligados deben garantizar el derecho de acceso a la información del particular, proporcionando la información con la que cuentan en el formato en que la*

misma obre en sus archivos; sin necesidad de elaborar documentos ad hoc para atender las solicitudes de información.

Sin más por el momento, reciba un cordial saludo.

Asimismo, **la Unidad de Informática**, en fecha **06 de noviembre de 2024**, mediante oficio número **TEEG-UI-74/2024**, hace de su conocimiento lo siguiente:

Por medio del presente y en relación con la solicitud de información pública que se presentó mediante la Plataforma Nacional de Transparencia con número de folio 110200200012224, de fecha 30 de octubre del presente año y en donde se solicita a esta Unidad de Informática lo siguiente:

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

El Tribunal como una institución pública se rige por normas de carácter general y local, por ende, se hace de su conocimiento que el término "gobierno de la seguridad" de manera amplia se refiere al conjunto de procesos, prácticas y políticas que controlan la gestión de la seguridad de la información, cuyo principal objetivo es establecer estrategias y normativa necesaria para proteger los activos de la información, lo cual, en términos de la Ley General de Datos Personales en Posesión de Sujetos Obligados y la ley local en la materia se relacionan con el sistema de gestión y Documento de Seguridad.

Por lo tanto, se han identificado estrategias, programas de capacitación y sensibilización, así como la elaboración del anteproyecto de Documento de Seguridad.

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).*

El Tribunal cuenta con un inventario físico de bienes informáticos de TIC; asimismo, se menciona que cada área es responsable del resguardo y respaldo de su información, por lo que, en caso de un

desastre, de manera inicial, se debe contar con los respaldos necesarios para la continuidad de la operación institucional; de igual forma, se cuenta con un anteproyecto de Documento de Seguridad y diversas acciones que inciden en la detección y planificación de medidas para la gestión de vulnerabilidades.

Por otra parte, este Tribunal cuenta con una política informática donde se derivan las responsabilidades de cada persona y área, implementada a partir del año 2023, así como la identificación de diversos procesos institucionales, a través de las fichas técnicas de valoración documental, que integran el Catálogo de Disposición Documental (CADIDO del Tribunal y en cuanto a activos se tiene un inventario de bienes informáticos, por lo que es, lo que se tiene implementado de lo que se menciona en la solicitud.

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;*

Actualmente la Unidad de Informática se encuentra en proceso de planificación de dicha temática a partir de la capacitación al personal de tecnologías de la información en esta materia, que permita establecer de manera integral aquellos aspectos necesarios para su consolidación.

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

En este punto se informa que, para algunos procesos, sí se emplea la firma electrónica avanzada.

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

Como ya se señaló, el Tribunal al ser una institución pública se rige por normas de carácter general y local, siendo el Pleno la máxima autoridad quien de acuerdo a los artículos 164, fracción XIX de la Ley de Instituciones y Procedimientos electorales para el Estado de Guanajuato y 10 fracción X del Reglamento Interior del Tribunal, tiene la atribución para llevar a cabo las acciones que estime necesarias para el buen funcionamiento de éste, inclusive para emitir cualquier tipo de disposición, sin que a la fecha se haya estimado necesario llevar a cabo acciones en dicha materia.

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;*

La seguridad de la información es atendida por la Unidad de Informática, en colaboración de diversas áreas del Tribunal, por lo que, a la fecha de la presente respuesta no se ha efectuado una contratación de esa naturaleza.

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

En el caso del Tribunal, se cuenta con los señalados en la primera y tercera hipótesis del cuestionamiento.

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.*

Sí se cuenta con lo señalado en el cuestionamiento.

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

Se realizan por parte de esta Unidad campañas de concientización sobre los ataques por phishing, vulnerabilidades por correos electrónicos fraudulentos y otras más por errores de los usuarios, además de que se realizan periódicamente revisiones y mantenimiento correctivo y preventivo.

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

Sí se cuenta con lo señalado en el cuestionamiento.

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

El personal de la Unidad de informática se encuentra actualmente en capacitación de ciberseguridad para la implementación de los protocolos necesarios en la institución, mismos que cuentan con las temáticas a las que hace referencia ese protocolo.

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;*

Como ya se señaló, el área se encuentra planificando la implementación de controles e indicadores en materia de seguridad de la información y realizando monitoreos continuos, con el objetivo de observar y registrar actividades en la red, detectando posibles amenazas o anomalías que pudieran indicar algún incidente de seguridad.

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.*

Con relación a dicho tema, se han llevado a cabo capacitaciones en temas de ciberseguridad para la protección de las bases de datos y los sistemas que albergan datos sensibles de la institución.

14. *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?;*

La respuesta a esta pregunta no corresponde a esta área.

15. *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, 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);*

La respuesta a esta pregunta no corresponde a esta área.

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 artículos 40, 41 y 42 de la Ley general de protección de datos personales en posesión de sujetos obligados (LGPDPPSO);*

La respuesta a esta pregunta no corresponde a esta área.

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

Se deben seguir las reglas marcadas en los lineamientos informáticos del Tribunal, los cuales están disponibles para su consulta en la liga electrónica siguiente:
https://teegto.org.mx/documentos/2024/normativa/Lineamientos%20Informaticos%202024.pdf

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.*

La respuesta a esta pregunta no corresponde a esta área.

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

No se han tenido incidencias representativas.

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

La respuesta a esta pregunta no corresponde a esta área.

21. *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;*

La respuesta a esta pregunta no corresponde a esta área.

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

La respuesta a esta pregunta no corresponde a esta área.

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

Se deben seguir las reglas marcadas en los lineamientos informáticos del Tribunal ya mencionados y se cuenta con los canales de comunicación como correo electrónico institucional o mensajería telefónica, en su defecto aquellos que valide el Pleno para esa finalidad.

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

Se actualizan de conformidad con las reglas marcadas en los lineamientos informáticos del Tribunal ya mencionados.

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

La respuesta a esta pregunta no corresponde a esta área.

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*

Las incidencias se gestionan de conformidad con las reglas marcadas en los lineamientos informáticos del Tribunal ya mencionados.

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)*

El Tribunal cuenta con infraestructura propia de seguridad, además de que no se han tenido incidencias representativas.

Esperando que la repuesta sea de utilidad, sin otro particular le envió un cordial saludo.

Finalmente, **la Unidad de Transparencia**, hace de su conocimiento lo siguiente:

Respecto de la pregunta identificada con el número **9**, se comunica que, de conformidad con la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Guanajuato, este Tribunal ha implementado diversas estrategias y mecanismos que inciden directamente en la prevención de la divulgación no autorizada de datos personales o información institucional, entre estas medidas se encuentran las siguientes:

- **Capacitación y sensibilización**: se ha llevado a cabo la capacitación continua con las personas servidoras públicas, sobre la importancia de proteger los datos, aspectos legales de su divulgación, y las mejores prácticas en protección de datos personales y ciberseguridad.
- **Implementación y adecuación del marco normativo:** El 26 de enero de 2021 se publicó en el Periódico Oficial del Gobierno del Estado de Guanajuato, el *Reglamento de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Tribunal Estatal Electoral de Guanajuato*[1], con el objeto de normar las disposiciones de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Guanajuato, así como las de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Guanajuato.
  En 2023, se aprobaron los "*Criterios específicos para la protección de datos personales en posesión del Tribunal Estatal Electoral de Guanajuato".*
- **Campañas de difusión en materia de protección de datos personales:** con el objetivo de impulsar y promover la conciencia y el conocimiento sobre la importancia de proteger los datos personales y garantizar el cumplimiento de las normativas en esta materia, se llevó a cabo la campaña denominada **#EL PODER DE MIS DATOS LO TENGO YO**, a través de la cual se buscó que las personas servidoras públicas, usuarias y cualquier persona involucrada en el tratamiento de datos personales comprendan y apliquen buenas prácticas para el resguardo, tratamiento y confidencialidad de la información.
  Referida campaña fue difundida a través de las redes sociales oficiales y se encuentra disponible en la página de internet, en el apartado de Datos Personales:
  https://transparencia.teegto.org.mx/datos_personales.html

En lo que corresponde al cuestionamiento número **10**, se informa que la página oficial de internet de este organismo jurisdiccional electoral, (https://www.teegto.org.mx) si cuenta con avisos de privacidad, tanto integrales como simplificados, los cuales están disponibles en:
https://transparencia.teegto.org.mx/datos_personales.html

[1] *https://periodico.guanajuato.gob.mx/downloadfile?dir=anio_2021&file=PO_18_2da_Parte_20210126.pdf*

Relativo a la interrogante identificada con el número **14**, se precisa que, el artículo 50 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Guanajuato, a la letra señala lo siguiente:

Sistema de gestión y documento de seguridad

Artículo 50. Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión.

*Se entenderá por **sistema de gestión** al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, de conformidad con lo previsto en la presente Ley y las demás disposiciones que le resulten aplicables en la materia.*

Por lo tanto, se deduce que, este Tribunal cuenta, de inicio, con un sistema de gestión en materia de protección de datos personales, pues tal como se ha señalado en diversas respuestas a sus planteamientos, se han realizado diferentes actividades que se interrelacionan e inciden en el tratamiento y seguridad de los datos personales en posesión de esta institución.

Por lo que, en observancia del numeral 13 de la ley en cita, este órgano electoral ha dado cumplimiento a los principios generales de protección de datos personales:

Principios generales de protección de datos personales

*Artículo 13. En todo tratamiento de datos personales que efectúe el responsable deberá observar los principios de **licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad.***

Puesto que se han diseñado elementos para asegurar su cumplimiento y garantizar la protección de datos personales, la privacidad y el fortalecimiento institucional, de entre algunos elementos claves, se han realizado las siguientes acciones:

- Emisión del Reglamento de Transparencia, Acceso a la Información Pública y **Protección de Datos Personales** del Tribunal Estatal Electoral de Guanajuato
- Programas de capacitación y sensibilización
- Avisos de privacidad simplificados e integrales
- Atención del ejercicio de los Derechos ARCOP
    - Realización del “Manual para ejercer los Derechos ARCOP”, disponible en: https://transparencia.teegto.org.mx/documentos/2024/manual_ARCOP.pdf
    - Realización del “Formato de solicitud de Derechos ARCOP”, disponible en: https://transparencia.teegto.org.mx/documentos/2024/formato_ARCOP.pdf
- Emisión de los *“Criterios específicos para la protección de datos personales en posesión del Tribunal Estatal Electoral de Guanajuato”*
- Análisis sobre la viabilidad de realización de evaluaciones de impacto en la protección de datos (EIPD)
- Anteproyecto de Documento de Seguridad del Tribunal Estatal Electoral de Guanajuato.

Ahora bien, respecto de su interrogante “desde cuando se adoptó y cuales áreas participaron en su desarrollo e implementación” (sic), se advierte que, para la conformación integral de dicho sistema de gestión, de los elementos plasmados con anterioridad, han sido diversas fechas en la cuales se han emitido o llevado a cabo las

actividades señaladas, sin embargo, usted podrá consultarlas directamente en los documentos proporcionados, de igual manera respecto de las áreas que han participado.

En lo tocante a las preguntas **15 y 16,** se precisa que, un modelo de comunicación para informar a la sociedad sobre incidentes de seguridad institucional y uno para notificar a las personas titulares de datos personales, en caso de brechas de seguridad en su información, tienen varias similitudes, pero también presentan diferencias clave en sus objetivos, enfoques y públicos específicos.

Por lo tanto, se hace de su conocimiento que este Tribunal no cuenta con un "modelo o sistema de comunicación para informar a la sociedad en general sobre sobre los eventos o incidentes de seguridad de la institución", o bien un "modelo o sistema de comunicación para informar a los titulares de datos personales en caso de brechas de seguridad de esta información" de manera particularizada o específica para esas finalidades.

No obstante, se hace la precisión de que este Tribunal cuenta con canales de comunicación oficiales que, de acuerdo con la naturaleza, objetivo de la comunicación, tipo de audiencia, tipo de información, serían utilizados, en caso de un incidente de seguridad institucional o brecha de seguridad en datos personales:

- La página web: www.teegto.org.mx
- Redes sociales: https://www.facebook.com/teegto.oficial X (antes Twitter) https://x.com/teegto y YouTube https://www.youtube.com/@teegto
- Plataforma Nacional de Transparencia: https://consultapublicamx.plataformadetransparencia.org.mx/vut-web/faces/view/consultaPublica.xhtml?idEntidad=MTE=&idSujetoObligado=MjAwMg==#inicio
- Correo electrónico institucional
- Líneas telefónicas institucionales

Así como aquellos que para su efecto se dispongan, por lo que, de conformidad con la legislación aplicable, en caso de alguna vulneración de seguridad, se procederá en los términos señalados en la normativa vigente. Tal como se establece en los artículos 54 al 58, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Guanajuato, que a la letra señalan lo siguiente:

Vulneraciones de seguridad

Artículo 54. Además de las que señalen las leyes respectivas y la normatividad aplicable, se considerarán como vulneraciones de seguridad, en cualquier fase del tratamiento de datos personales, al menos, las siguientes:
I. La pérdida o destrucción no autorizada;
II. El robo, extravío o copia no autorizada;
III. El uso, acceso o tratamiento no autorizado, o
IV. El daño, la alteración o modificación no autorizada.

Bitácora de vulneraciones de seguridad ocurridas

Artículo 55. El responsable deberá llevar una bitácora de las vulneraciones a la seguridad ocurridas en la que se describa:

I. La fecha en la que ocurrió;
II. El motivo de la vulneración de seguridad, y

III. Las acciones correctivas implementadas de forma inmediata y definitiva.

Notificación de las vulneraciones de seguridad ocurridas

Artículo 56. El responsable deberá informar sin dilación alguna al titular y al Instituto las vulneraciones de seguridad ocurridas, que de forma significativa afecten los derechos patrimoniales o morales del titular, en un plazo máximo de setenta y dos horas en cuanto se confirmen, y haya empezado a tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, a fin de que los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos.

Contenido de la notificación de la vulneración

Artículo 57. El responsable deberá informar al titular y al Instituto, al menos, lo siguiente:
I. La naturaleza del incidente;
II. Los datos personales comprometidos;
III. Las recomendaciones y medidas que el titular puede adoptar para proteger sus intereses;
IV. Las acciones correctivas realizadas de forma inmediata, y
V. Los medios donde puede obtener mayor información al respecto.

Implementación de acciones correctivas y preventivas ante una vulneración de seguridad

Artículo 58. En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales si fuese el caso, a efecto de evitar que la vulneración se repita.

Al respecto, y en atención al cuestionamiento número **18** se indica que la información curricular desde el nivel de jefatura de departamento o equivalente, hasta el titular del sujeto obligado, de este Tribunal se encuentra disponible en la PNT, toda vez que se trata de una obligación de transparencia, de acuerdo con el artículo 26, fracción XVII, de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Guanajuato.
Es entonces que usted podrá consultarla directamente en referida plataforma, donde podrá encontrar entre otros datos, el puesto, área de adscripción, nivel máximo de estudios, carrera genérica y experiencia laboral, disponible en el vínculo siguiente:
https://consultapublicamx.plataformadetransparencia.org.mx/vut-web/faces/view/consultaPublica.xhtml?idEntidad=MTE=&idSujetoObligado=MjAwMg==#inicio

Sobre la pregunta número **20**, referente a la adopción de esquemas de mejores prácticas en materia de protección de datos personales, se indica que, a la fecha de la presente respuesta, los esquemas a los que hace referencia (ej., cifrado de datos, anonimización, seudonimización, privacidad desde el diseño, oficial de datos personales, auditorías voluntarias, etc.) no han sido documentados en esta institución.

En lo tocante a la pregunta **21,** se hace de su conocimiento que este tribunal electoral cuenta con diversos sistemas informáticos y plataformas digitales que, pudieran implicar un tratamiento de datos personales, en este tenor, me permito señalar que se encuentran en operación y funcionamiento, y no en todos los casos, se implica

el manejo intensivo o relevante de carácter general y/o particular de datos personales, por lo tanto, se considera una exención la elaboración de una Evaluación de Impacto a la Protección de Datos Personales (EIPD)[2]

Aunado a lo anterior, es preciso señalar que únicamente algunos de los sistemas han sido desarrollos de este sujeto obligado, pues a través de convenios con diversas instituciones públicas, han sido donados algunos otros, lo que los excluye de la elaboración de la EIPD por parte de este órgano electoral, ya que esta debe realizarse desde el diseño del sistema informático o plataforma digital.

Ahora bien, para el caso concreto de la Plataforma Electrónica Electoral Local (PEEL), la cual pudiera implicar un tratamiento intensivo y/o relevante de datos personales, fue puesta en marcha en años anteriores, y a la fecha no ha sido modificada, ni se pretende realizar alguna actualización a un corto plazo, por lo que, no se encuentra en el supuesto de la realización de una EIPD de manera retroactiva.

Referente a la interrogante **22,** se indica que, de conformidad con el artículo 3, fracción XII de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Guanajuato, el **documento de seguridad** es un instrumento que describe y da cuenta de manera general sobre las medidas de seguridad de carácter técnico, físico y administrativo adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

En este sentido, me permito señalar que en los últimos ejercicios se han implementado diversas acciones tendientes al desarrollo del instrumento en referencia, por lo que se elaboró **un anteproyecto de Documento de Seguridad**, el cual requiere ser presentado por la Unidad de Transparencia, para su revisión, análisis, y en su caso, aprobación del Comité de Transparencia, para su posterior remisión al Pleno de este Tribunal, a fin de ser emitida, y autorizada su publicación, una vez realizadas las adecuaciones que se consideren pertinentes.

Vale la pena señalar que, de acuerdo con la **Guía de apoyo para la elaboración del Documento de Seguridad** del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), publicada en diciembre de 2022, las etapas a desarrollar son las siguientes:

1. Inventario de datos y sistemas de tratamiento.
2. Funciones y obligaciones de las personas que traten datos personales.
3. Análisis de riesgos.
4. Análisis de brecha.
5. Plan de trabajo.
6. Mecanismos de monitoreo y revisión de las medidas de seguridad.
7. Programa general de capacitación.

En este sentido, se detectó que uno de los elementos indispensables para el desarrollo y ejecución de la etapa 1, era mencionar el plazo de conservación de los datos personales:

[2] De acuerdo con los numerales 3, fracción XVI de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Ley General), 3, fracción XIV, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Guanajuato (Ley de Datos de Guanajuato), y 6 de las Disposiciones Administrativas de Carácter General para la Elaboración, Presentación y Valoración de Evaluaciones de Impacto en la Protección de Datos Personales (Disposiciones administrativas); se trata de un documento de análisis mediante el cual los responsables del tratamiento de datos personales del sector público valoran los impactos reales respecto de un tratamiento intensivo o relevante de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes, derechos y demás obligaciones en materia aplicable y fomentar una cultura de protección de datos personales al interior de la organización del responsable.

ETAPA 1. EL INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO.
Mencionar el plazo de conservación de los datos personales.

*"**Este plazo tendría que estar definido en los instrumentos de clasificación archivística**. Por ello es necesario identificar a qué serie documental pertenecen los archivos o bases de datos en los que están contenidos los datos personales. Una vez que se haya realizado un diagnóstico en materia archivística, estará preparado para cumplir de mejor modo las obligaciones previstas en la Ley General y los Lineamientos Generales".*

Al respecto se precisa que dichos plazos se encuentran vinculados con los plazos y vigencias establecidos en el *Catálogo de Disposición Documental (CADIDO),* instrumento de control validado por el Grupo Interdisciplinario de Archivos de este Tribunal, en la Primera Sesión Ordinaria iniciada el 25 de enero de 2024 y clausurada el 01 de febrero de la misma anualidad, siendo remitido al Pleno para su aprobación.

Por lo tanto, una vez consolidado el anteproyecto por parte del Comité de Transparencia, y aprobado por el Pleno, la versión pública del Documento de Seguridad, la podrá consultar en la página de Internet de este sujeto obligado https://www.teegto.org.mx/

Se da por notificada la presente respuesta a la solicitud de acceso a la información pública, de conformidad con lo establecido en los artículos 85 y 99 de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Guanajuato.

Atentamente

Mtra. María Dolores Serrano Luna
Titular de la Unidad de Transparencia