



**TRIBUNAL ELECTORAL DEL ESTADO  
DE JALISCO**

**SOLICITUD DE INFORMACIÓN**  
TEEJ-INFO-185/2024

**SOLICITANTE:**  
Qt

**ASUNTO:**  
Se da respuesta.

Guadalajara, Jalisco, a 12 doce de noviembre de 2024 dos mil veinticuatro.

**Vista** la solicitud de información formulada de manera anónima, misma que fue presentada vía Plataforma Nacional de Transparencia, generando el folio 140279524000121 y recibida oficialmente el día 31 treinta y uno de noviembre de 2024 dos mil veinticuatro, en la cual solicita:

*"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 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. 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) " (sic)*

En ese orden de ideas, en virtud de que la solicitud de información reúne los requisitos contemplados en el artículo 79 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, se radica y se admite bajo el número de expediente **TEEJ-INFO-185/2024**, toda vez que esta Unidad de Transparencia resulta competente para recibir la presente solicitud de información. Lo anterior, para todos los efectos legales a que haya lugar.

Por otro lado, es esencial esclarecer que la Unidad de Transparencia es un área de trámite y gestión de solicitudes, por lo que solo requiere y recaba de las áreas internas de este sujeto obligado la información pública de las solicitudes procedentes, lo anterior, conforme al artículo 32, fracción VIII, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, sin que dicha Unidad sea la que resguarde de manera directa toda la información generada por el Tribunal Electoral del Estado de Jalisco.

Lo que se comunica para los efectos legales correspondientes, en los términos del artículo 135 fracción III del Reglamento Interno del Tribunal Electoral del Estado de Jalisco, en relación a los artículos 3, 8, 11-Bis, 24, fracción X, 31 y 32, así como los demás relativos a la Ley de la materia.

Ahora bien, esta Unidad de Transparencia efectuó las gestiones internas necesarias para solventar dicha solicitud de información, girando oficio **UTI-TEEJ-202/2024**, al Departamento de Control de Patrimonio; **UTI-TEEJ-203/2024**, al Departamento de Comunicación Social; **UTI-TEEJ-204/2024**, al Departamento de Recursos Materiales; **UTI-TEEJ-205/2024**, a la Oficina de Informática; **UTI-TEEJ-206/2024**, a Dirección de Administración y **UTI-TEEJ-207/2024**, a la Oficina de Jurídico, todos

de este Tribunal Electoral, quienes dieron respuesta en el ámbito de su competencia, en los siguientes términos:



OFICIO No. CAOC-TEAD-101/2024  
Guadalajara, Jalisco a 06 de noviembre de 2024

Lic. César Octavio Magallanes Escalera  
Titular de la Unidad de Transparencia y Protección de Datos Personales  
del Tribunal Electoral del Estado de Jalisco.  
Presente

En atención al oficio identificado con la clave UTI-TEEJ-206/2024, mediante la cual me informa sobre la solicitud de información Pública, la cual se tramita bajo el expediente administrativo TEEJ-INFO-185/2024 al respecto se informa lo siguiente:

4. Informar si se emplea la firma electrónica en la Institución;

Respecto a lo requerido en el punto 4 de la referida solicitud, le informo, que este Tribunal Electoral del Estado de Jalisco cuenta con firma electrónica avanzada para realizar trámites de carácter administrativo ante el Servicio Administración de Tributaria SAT, así como para la emisión de facturas y declaración de impuestos.

Asimismo, este sujeto obligado hace uso de la Firma Electrónica Avanzada en los procesos de fiscalización y redición de cuentas, en el Sistema de Control, Administración y Fiscalización de los Recursos del Gasto Federalizado (SiCAF), de conformidad a lo establecido en la Ley de Fiscalización y Rendición de Cuentas de la Federación.

Así pues, en términos de lo dispuesto por el artículo 68 de la Constitución Política del Estado de Jalisco, el Tribunal Electoral del Estado de Jalisco es un organismo público autónomo, con personalidad jurídica y patrimonio propios, con autonomía técnica y de gestión en su funcionamiento e independiente en sus decisiones y que se rige bajo los principios de certeza, imparcialidad, objetividad, legalidad y probidad.

Atentamente  
"2024, Año del Bicentenario del Nacimiento del Federalismo Mexicano,  
así como de la Libertad y Soberanía de los Estados"

Carlos Alberto Olvera Govearrubias  
Director General de Administración







TERM-016/2024

**LIC. CÉSAR OCTAVIO MAGALLANES ESCALERA**  
Unidad de Transparencia y Protección de Datos Personales  
del Tribunal Electoral del Estado de Jalisco.  
Presente

En atención al oficio identificado con la clave UTI-TEEJ-204/2024, mediante la cual me informa sobre la solicitud de información pública presentada mediante la Plataforma Nacional de Transparencia generando el Número de folio 1402795224000121, misma que se tramita bajo el expediente administrativo TEEJ-INFO-185/2024 y que solicita saber lo siguiente:

**Pregunta 2.- Señalar si cuenta con lo siguiente: a) Un marco de mejores practicas aplicables a la gestion de las TIC en los diferentes procesos de contratacion para la adquisicion, el arrendamiento de bienes o la prestacion de servicios en materia TIC y de seguridad de la informacion.**

En referencia a la solicitud hecha, le menciono que todas las compras que se han realizado a través de Licitación, Adjudicaciones Directas y fondos, se han hecho bajo estricto apego a la ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios y los Lineamientos de Adquisiciones, Enajenaciones, Arrendamientos y Servicios del Tribunal Electoral del Estado de Jalisco.

De igual manera le informo que de algunas mejoras que se han realizado en los procesos de Contratación para la adquisición de bienes, arrendamientos o prestación de servicios son:

1. En algunos casos se tienen más cotizaciones de las que indica la ley, con la finalidad de garantizar una buena adquisición, analizando diferentes rubros: calidad, costo, tiempo de entrega.
2. En algunas Licitaciones, en las que se adjudica de manera directa, participa un solo proveedor y se le solicita que entregue su documentación, aunque se solicite posteriormente requisiciones para el proceso de Adjudicación, con la finalidad de darle más certeza al proceso en el que se declara desierta la misma por no tener dos propuestas para análisis.



Con esta participación se analiza también la importancia e interés que tiene el proveedor al acudir al proceso.

Sin más por el momento, quedo a sus órdenes para cualquier duda o aclaración.

Atentamente  
Guadalajara, Jalisco a 06 de noviembre de 2024.

**C. RICARDO LOMELI FAMOSO**  
Jefe de Departamento de Recursos Materiales  
del Tribunal Electoral del Estado de Jalisco





TECP-009/2024

**LIC. CÉSAR OCTAVIO MAGALLANES ESCALERA**  
Unidad de Transparencia y Protección de Datos Personales  
del Tribunal Electoral del Estado de Jalisco.  
Presente

En atención al oficio identificado con la clave UTI-TEEJ-202/2024, mediante la cual me informa sobre la solicitud de información pública presentada mediante la Plataforma Nacional de Transparencia generando el Número de folio 1402795224000121, misma que se tramita bajo el expediente administrativo TEEJ-INFO-185/2024 y que solicita saber lo siguiente:

**Pregunta 2.- Señalar si cuenta con lo siguiente: Informar si cuenta con un inventario institucional de bienes y servicios de TIC.**

En referencia a la solicitud hecha le menciono que se le proporciona los Link's en los cuales se encuentra el inventario de bienes de este Órgano Jurisdiccional y en el que encontrara los recursos, herramientas, programas, equipos y medios que permiten procesar, almacenar transmitir y compartir información.

1. <https://www.triejal.gob.mx/transparencia/informacion-financiera-patrimonial-y-administrativa/inventarios/>
2. [https://www.recursos.triejal.gob.mx/contabilidad\\_gubernamental/RelBienesmueblesActivoene-jun-24.pdf](https://www.recursos.triejal.gob.mx/contabilidad_gubernamental/RelBienesmueblesActivoene-jun-24.pdf)

Sin más por el momento, quedo a sus órdenes para cualquier duda o aclaración.

Atentamente  
Guadalajara, Jalisco a 06 de noviembre de 2024.

LIC. CARLOS ALBERTO OLVERA GOWARRUBIAS  
DIRECTOR GENERAL DE ADMINISTRACIÓN DEL  
TRIBUNAL ELECTORAL DEL ESTADO DE JALISCO.



**J-TEEJ-038/2024**  
Se contesta solicitud de información.

**César Octavio Magallanes Escalera**  
Titular de la Unidad de Transparencia y  
Protección de Datos Personales del  
Tribunal Electoral del Estado de Jalisco  
Presente:

Aunado a un cordial saludo, y en atención a su oficio UTI-TEEJ-207/024, mediante el cual hizo del conocimiento de esta Jefatura Jurídica, la solicitud de información presentada mediante la Plataforma Nacional de Transparencia, la cual se tramita bajo el expediente administrativo interno TEEJ-INFO-185/2024, para su puntual respuesta.

Por lo anterior, y para que dicha Unidad esté en aptitud de dar respuesta en el plazo establecido en el artículo 84, párrafo 1 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios informo lo siguiente:

**Cuestionamientos:**

**Que realizan mediante un total de 17 cuestionamientos, numerados del 11 al 27 que en obvio de repeticiones se reproducen al presente:**

En lo que respecta a ésta Jefatura Jurídica del Tribunal Electoral del Estado de Jalisco se indica la siguiente:

**Respuesta:**

Dígasele al Solicitante de información que de conformidad a lo dispuesto por los artículos 68, de la Constitución Política del Estado de Jalisco y 2 de la Ley Orgánica del Tribunal Electoral del Estado de Jalisco, este sujeto obligado es un Organismo Público, Constitucional Autónomo, de carácter permanente, que se rige bajo los principios de certeza, imparcialidad, objetividad, legalidad y probidad. El cual tendrá a su cargo la función jurisdiccional local en materia electoral.

En relación a lo anterior cabe señalar, que al igual que los demás organismos jurisdiccionales, este Tribunal Electoral del Estado de Jalisco, se encuentra sujeto a la observancia de la totalidad de los principios que integran el derecho fundamental de impartición de justicia, entre el que destaca, en un sistema tradicional de conformidad a lo que dispone la Constitución Política de los Estados Unidos Mexicanos, la Constitución del



*[Handwritten signature]*





Estado de Jalisco, regulado mediante disposiciones procesales contenidas en el Código Electoral del Estado de Jalisco.

Por lo que, de sus cuestionamientos en lo particular al Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos, en razón, de indicado del párrafo anterior, el sistema de aplicación de justicia por parte del Tribunal, queda ajeno al sistema que se indica el citado Protocolo.

Cabe destacar con relación al cuestionamiento señalado con el número 54, se informa que, en el Tribunal, existe un medio electrónico, por medio del cual la Secretaría General de Acuerdos, por el cual turnan los asuntos a las Ponencias del Órgano Jurisdiccional.

Sin más por el momento le reitero mi entera disposición y compromiso en materia de transparencia por parte de esta Jefatura Jurídica.

ATENTAMENTE  
Guadalajara, Jalisco, 7 de noviembre de 2024.

Carlos Alejandro Díaz López.  
Titular de la Jefatura Jurídica



LIC. CÉSAR OCTAVIO MAGALLANES ESCALERA.  
JEFE DE DEPARTAMENTO DE LA UNIDAD DE TRANSPARENCIA Y  
PROTECCIÓN DE DATOS PERSONALES DEL TRIBUNAL ELECTORAL  
DEL ESTADO DE JALISCO.  
PRESENTE.

De conformidad a lo solicitado por el oficio UTI-TEEJ-203-2024 con fecha del 1 de noviembre del año en curso, le informo:

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

- En el Tribunal Electoral del Estado de Jalisco se realizan los simulacros establecidos en la normativa aplicable.
- <https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPC.pdf>
- [https://congresoweb.congresoal.gob.mx/BibliotecaVirtual/legislacion/Leyes/Documentos\\_PDF-Leyes/Ley%20de%20Protección%20Civil%20del%20Estado-230523.pdf](https://congresoweb.congresoal.gob.mx/BibliotecaVirtual/legislacion/Leyes/Documentos_PDF-Leyes/Ley%20de%20Protección%20Civil%20del%20Estado-230523.pdf)
- [https://www.diputados.gob.mx/LeyesBiblio/regley/Reg\\_LGPC\\_091215.pdf](https://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LGPC_091215.pdf)

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

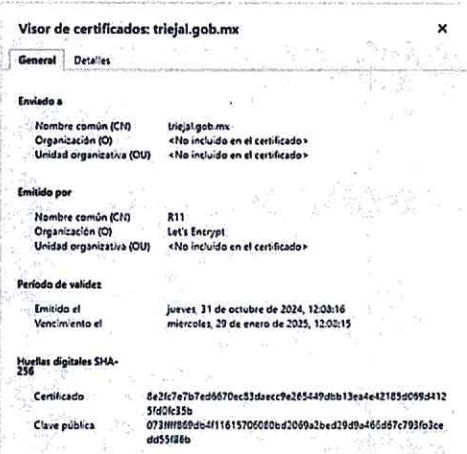
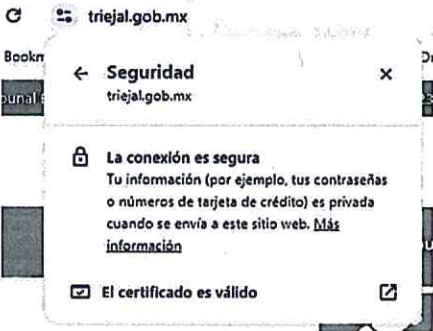
This is the certificate information for triejal.gob.mx.

Field	Value
Challenge Method	http-01
Id	triejal_gob_mx_df289_ab929_1738174095_f6581892320f3f0a6ca7eb3e92e34d4d
Order Url	https://acme-v02.api.letsencrypt.org/acme/order/42418245/318797536307
Subject	triejal.gob.mx
DNS Names	[mail.triejal.gob.mx triejal.gob.mx www.triejal.gob.mx]
Issuer	R11
Valid After	2024-10-31 18:08:16 +0000 UTC

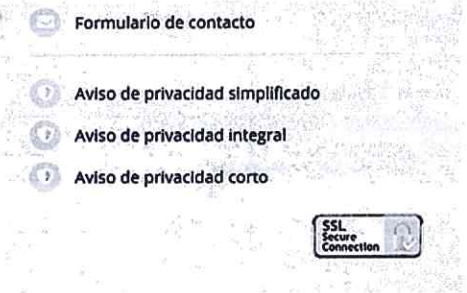


Valid Before 2025-01-29 18:08:15 +0000 UTC

La renovación de dicho certificado se gestiona desde consola de administración Linux (cPanel) y se actualiza dicho certificado de manera automática de manera mensual.



Así mismo cuenta con el aviso de privacidad en tres formatos distintos y señalando gráficamente que el sitio web cuenta con el certificado de seguridad al pie de página:



Señalar si las páginas web de los buscadores de versiones públicas de sentencias del Tribunal, tienen certificados digitales vigentes

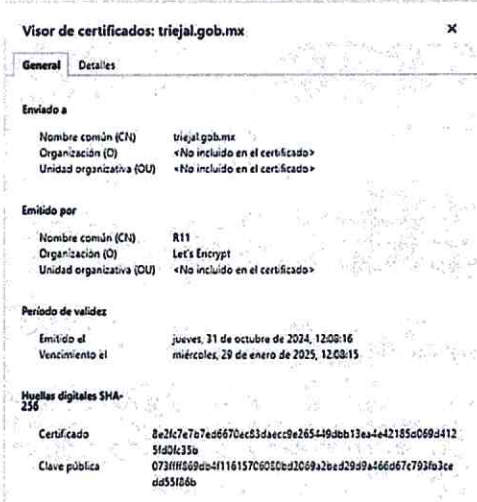
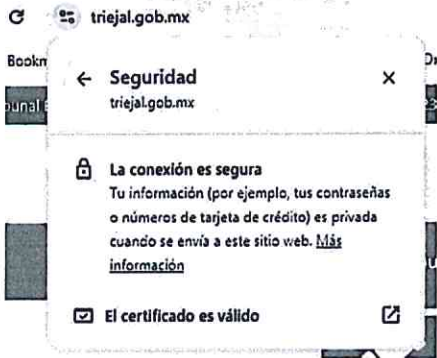
This is the certificate information for triejal.gob.mx.

Field	Value
Challenge Method	http-01
Id	triejal_gob_mx_df289_ab929_1738174095_f6581892320f3f0a6ca7eb3e92e34d4d
Order Url	https://acme-v02.api.letsencrypt.org/acme/order/42418245/318797536307
Subject	triejal.gob.mx
DNS Names	[mail.triejal.gob.mx triejal.gob.mx www.triejal.gob.mx]
Issuer	R11
Valid After	2024-10-31 18:08:16 +0000 UTC
Valid Before	2025-01-29 18:08:15 +0000 UTC

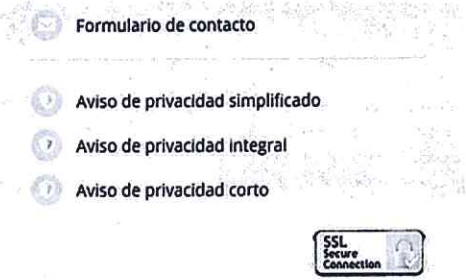
La renovación de dicho certificado se gestiona desde consola de administración Linux (cPanel) y se actualiza dicho certificado de manera automática de manera mensual.

Handwritten signature in blue ink.





Así mismo cuenta con el aviso de privacidad en tres formatos distintos y señalando gráficamente que el sitio web cuenta con el certificado de seguridad al pie de página:



Sin más por el momento reciba un cordial un saludo.

ATENTAMENTE  
Guadalajara, Jalisco, a 08 de noviembre del 2024.

LIC. JULIA MARÍA ELENA PRIETO BECERRA.  
JEFE DE OFICINA DE COMUNICACIÓN SOCIAL Y DIFUSIÓN.

c.c.p. Interesado



UNIDAD DE TRANSPARENCIA  
TRIBUNAL ELECTORAL DEL ESTADO DE JALISCO  
PRESENTE

En respuesta a su solicitud de información con referencia a su expediente administrativo TEEJ-INFO-185/2024 número de folio 1402795224000121 con gusto brindamos la respuesta correspondiente a los cuestionamientos numerados en apartado adjunto al mismo.

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

R) En nuestra institución, se cuenta con un Documento de Seguridad: [https://www.triejal.gob.mx/documento\\_de\\_seguridad/](https://www.triejal.gob.mx/documento_de_seguridad/), donde se implica la participación de todas las áreas que la conforman.

2. Señalar si se cuenta con lo siguiente: a) un marco de mejores prácticas aplicables a la gestión de las TIC en los diferentes procesos de contratación para la adquisición, el arrendamiento de bienes o la prestación de servicios en materia de TIC y de seguridad de la información; 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) o Sistema de Gestión de Seguridad de la Información (SGSI); g) Informar si se cuenta con una política general de seguridad de la información y en su caso, quienes intervienen y desde cuándo se implementó; h) Informar si se cuenta con un diagnóstico de identificación de los procesos y activos esenciales de la institución; i) Informar si se cuenta con un Equipo de Respuesta a Incidentes de Seguridad de la Información (ERISC) o Equipo de respuesta a Incidentes Cibernéticos o en su caso SOC.

R) La coordinación para la adquisición de nuevas implementaciones acordes a las necesidades de ciberseguridad así como adquisición de bienes y servicios, implica la participación de todos los departamentos que conforman el Tribunal Electoral del Estado de Jalisco, tomando como base nuestro Documento de Seguridad.

En el DEPARTAMENTO DE INFORMATICA hemos previsto como estrategia el respaldo en medios electrónicos de toda la información en nuestros servidores electrónicos, nuestro inventario de equipos de computo se mantiene constantemente actualizado y resguardado debidamente así como la información procesada en nuestros equipos. [https://www.triejal.gob.mx/documento\\_de\\_seguridad/](https://www.triejal.gob.mx/documento_de_seguridad/)

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;

R) Se ha instruido al personal de las distintas áreas, Jurídico, Administración, Actuaría, Control Patrimonial, Contabilidad, Planeación, Secretaría General, Oficialía de partes, Órgano Interno de Control, Recursos Humanos, Comunicación Social, así como también Área de Informática, para que toda la información generada, sea respaldada en dispositivos electrónicos bajo resguardo del DEPARTAMENTO DE INFORMATICA.





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

R) Si, Es un instrumento utilizado principalmente en áreas administrativas y contables.

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

R) Mensualmente el DEPARTAMENTO DE INFORMÁTICA, realiza una revisión y respaldo de nuestra información por cada uno de nuestros servidores electrónicos en la red interna de esta institución

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 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

R) Todas las gestiones para la adquisición de nuevas tecnologías son protocolizadas mediante una licitación considerando los lineamientos oficiales de gobierno apegados a nuestras necesidades de actualización, considerando lo descrito en nuestro Documento de Seguridad, [https://www.triejal.gob.mx/documento\\_de\\_seguridad/](https://www.triejal.gob.mx/documento_de_seguridad/)

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

R) El equipamiento electrónico utilizado como central de datos es operado por personal del DEPARTAMENTO DE INFORMATICA y es propiedad de nuestra propia institución.

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 o en su caso de transparencia y acceso a la información; c) control institucional de la totalidad de los correos contenidos en las carpetas de los usuarios; d) Soluciones de filtrado para correo no deseado o correo no solicitado, así como programas informáticos que protejan del envío y recepción de correos electrónicos con software malicioso; e) cuenta con cifrado en el envío de información.

R) El personal encargado de cada área de trabajo, cuenta con correo institucional, registrado a su nombre mismo que cuenta con un apartado de SPAM.

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

R) El Tribunal Electoral del Estado de Jalisco cuenta con un documento de seguridad que establece las medidas físicas y tecnológicas para este fin, mismas que pueden ser consultadas en el siguiente vínculo electrónico. [https://www.triejal.gob.mx/documento\\_de\\_seguridad/](https://www.triejal.gob.mx/documento_de_seguridad/)



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

R) Cumple con ambos Incisos

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

R) Todo el personal implicado es instruido para considerar en cualquier incidente lo instruido en nuestro Documento de Seguridad publicado en; [https://www.triejal.gob.mx/documento\\_de\\_seguridad/](https://www.triejal.gob.mx/documento_de_seguridad/)

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 la madurez institucional en la gestión de seguridad de la información;

R) Todos los mecanismos utilizados para control, evaluación y medición necesarios son en base a nuestro Documento de Seguridad publicado en; [https://www.triejal.gob.mx/documento\\_de\\_seguridad/](https://www.triejal.gob.mx/documento_de_seguridad/)

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.

R) Se cuenta con un Documento de Seguridad Publicado en; [https://www.triejal.gob.mx/documento\\_de\\_seguridad/](https://www.triejal.gob.mx/documento_de_seguridad/)

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

R) Se aplican los controles y mecanismos de seguridad para la transferencia de documentos y cualquier dispositivo mencionados en el documento de seguridad publicado en nuestro portal de internet, [https://www.triejal.gob.mx/documento\\_de\\_seguridad/](https://www.triejal.gob.mx/documento_de_seguridad/)

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

R) Ningún incidente asta esta fecha ha sido registrado.

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;

R) Ningún tratamiento intensivo ha sido requerido puesto que por lo general solo utilizamos procesadores de datos y hoja de cálculo.





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

R) Por protocolo, la información comprometida es contenida y resguardada por el DEPARTAMENTO DE INFORMATICA y reportada mediante un procedimiento administrativo a la Dirección de Administración del Tribunal Electoral del Estado de Jalisco.

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

R) Si se encuentra publicado en; [https://www.triejal.gob.mx/documento\\_de\\_seguridad/](https://www.triejal.gob.mx/documento_de_seguridad/)

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

R) Las medidas de seguridad cibernética se revisan por el DEPARTAMENTO DE INFORMATICA y son verificados diariamente.

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

R) Esta institución opera de manera autónoma y realiza revisión interna de sus operaciones mediante el DEPARTAMENTO DE INFORMATICA conforme a su Documento de Seguridad; [https://www.triejal.gob.mx/documento\\_de\\_seguridad/](https://www.triejal.gob.mx/documento_de_seguridad/)

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

R) Cualquier incidente se reporta de manera personal al DEPARTAMENTO DE INFORMATICA ya sea telefónicamente o por escrito.

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)

R) Todo incidente que implique ciberseguridad, será centralizado en el DEPARTAMENTO DE INFORMATICA y canalizado mediante informe oficial dirigido al encargado del departamento afectado, de acuerdo a nuestro Documento de Seguridad.



ATENTAMENTE

Guadalajara, Jalisco a 11 de noviembre de 2024

ING. ALBERTO VÁZQUEZ MORENO

AUXILIAR ADMINISTRATIVO DEPARTAMENTO DE INFORMATICA  
TRIBUNAL ELECTORAL DEL ESTADO DE JALISCO

De igual forma y tal como se desprende del oficio del Jefe de la Oficina de Jurídico de este Órgano Jurisdiccional y privilegiando los principios de transparencia y máxima publicidad, se hace de su conocimiento que de los principios que integran el derecho fundamental de impartición de justicia, destaca en este Tribunal Electoral del Estado de Jalisco un sistema tradicional de conformidad a lo que dispone la Constitución Política de los Estados Unidos Mexicanos, la Constitución del Estado

Libre y Soberano de Jalisco y regulado por las disposiciones procesales contenidas en el Código Electoral del Estado de Jalisco.

Ahora bien, en lo que respecta parte del **cuestionamiento en relación al correo electrónico institucional**, este Tribunal Electoral del Estado de Jalisco, si implementa dicha leyenda, que a la letra dice:

*"El contenido de este correo electrónico es información pública y susceptible de una solicitud de información".*

*"Ahorra energía y papel, si no es necesario no imprimas este correo".*

De igual manera, cuando se transfiere información confidencial a Autoridad diversa y en cumplimiento a lo estipulado en Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, se le agrega a dicha transferencia constancia de protección de datos, misma que se anexa a este documento.

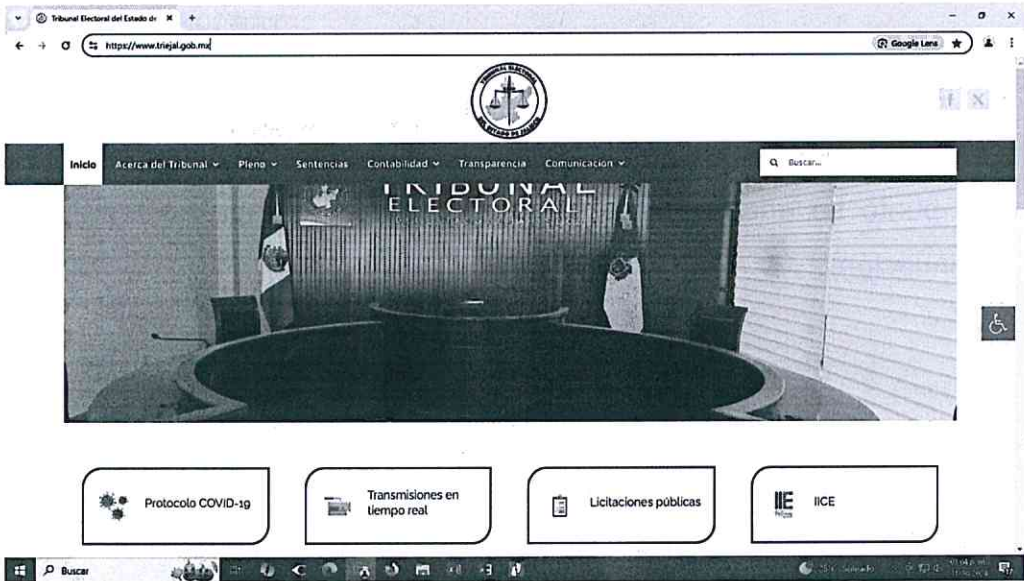
Así mismo, en lo que respecta al **cuestionamiento evitar la divulgación no autorizada de datos o información Institucional**, se le comunica que la versión pública del documento de seguridad, puede consultarse y descargarse en el siguiente link correspondiente a la página oficial de este Sujeto Obligado:

[https://www.triejal.gob.mx/documento\\_de\\_seguridad/](https://www.triejal.gob.mx/documento_de_seguridad/)

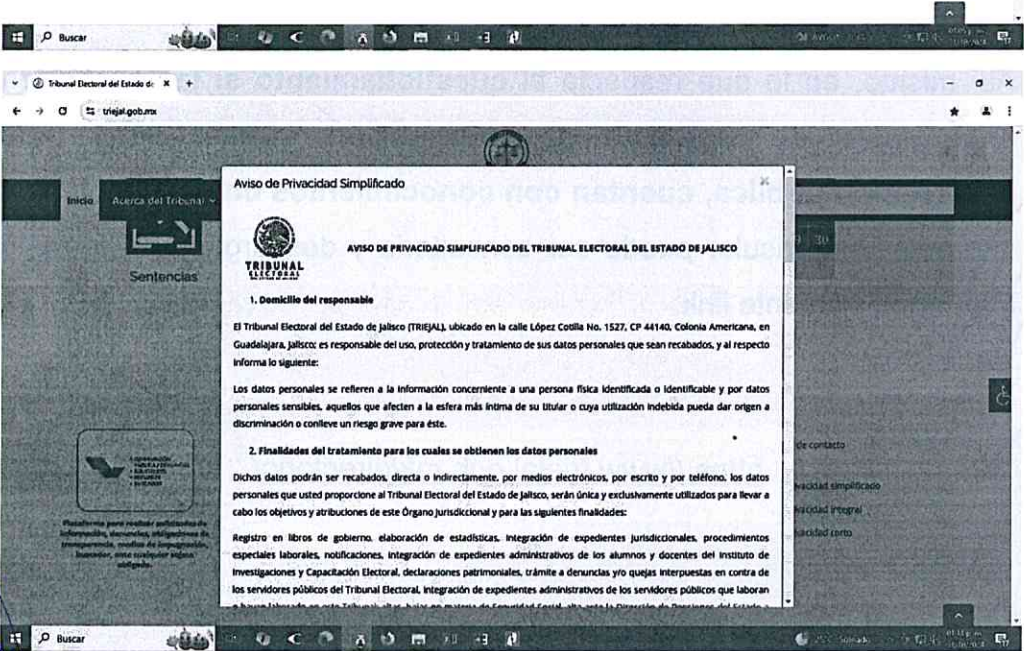
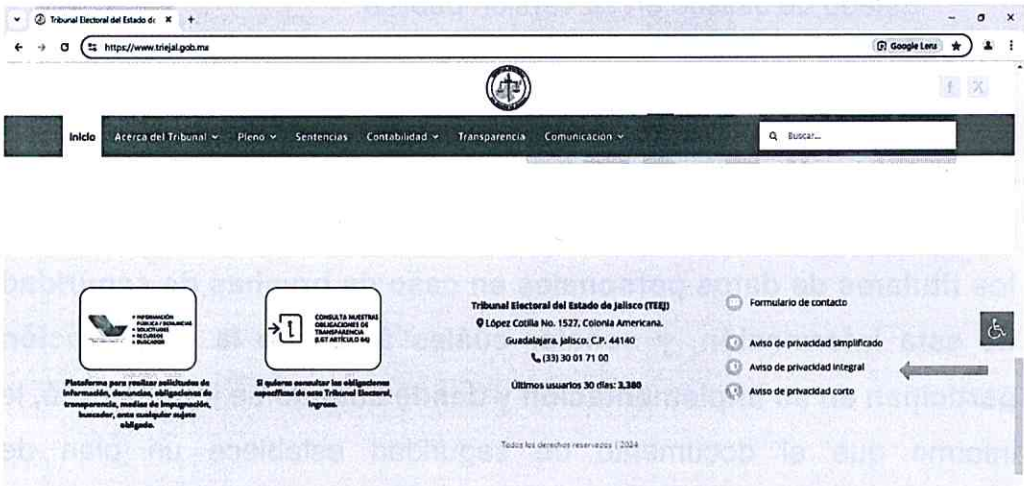
En lo que respecta parte del **cuestionamiento relacionado con el aviso de privacidad**, puede ser consultado en la página oficial de este Sujeto Obligado de la siguiente manera:

<https://www.triejal.gob.mx/>





Se pueden encontrar los diversos avisos de privacidad en la parte inferior derecha, al dar *click* sobre ellos, se despliega el documento:



Por lo que respecta al **cuestionamiento sobre si se cuenta con un sistema de gestión de protección de datos personales**, en relación a este punto se anexa al presente los documentos que se enlistan a continuación:

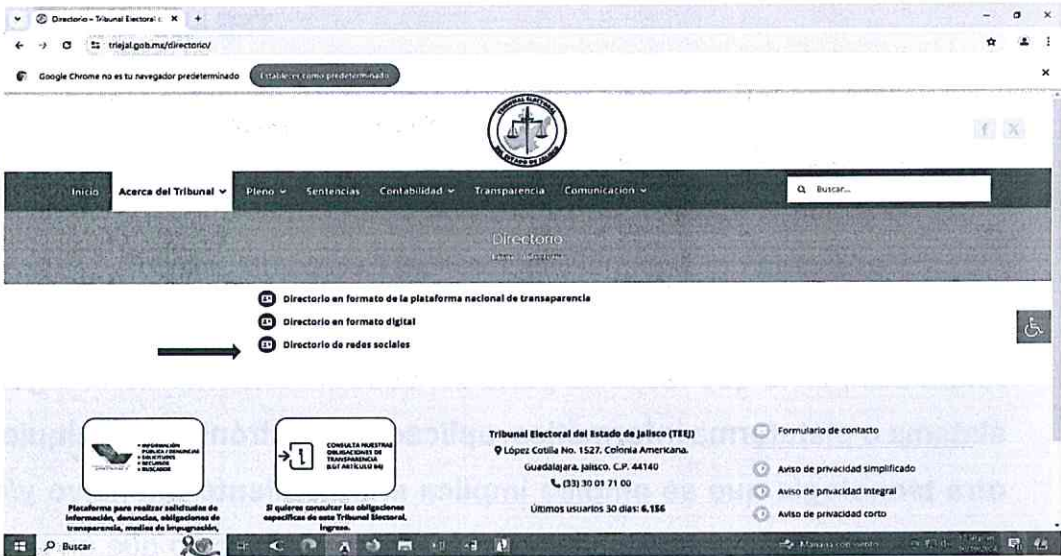
1. Políticas Internas de Gestión y Tratamiento de Datos Personales del Tribunal Electoral del Estado de Jalisco.
2. Criterios Generales de Protección de Información Confidencial y Reservada del Tribunal Electoral del Estado de Jalisco.
3. Documento de Seguridad del Tribunal Electoral del Estado de Jalisco en su versión pública.

Ahora bien, en lo que respecta parte del **cuestionamiento 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**, le informo que el documento de seguridad establece un plan de contingencia para la protección de la información de este sujeto obligado.

Así mismo, en lo que respecta al **cuestionamiento si las personas encargadas de sistemas de información, donde se brinde información pública, cuentan con conocimientos comprobables**, la información curricular puede ser consultada y descargada en formato PDF en el siguiente link:

<https://www.triejal.gob.mx/directorio/>





Al darle entrar a “Directorio en formato digital”, se descargará un archivo en Excel, en donde podrá acceder a la información curricular del titular de la Unidad de Transparencia y Protección de Datos Personales de este Tribunal Electoral del Estado de Jalisco:

	TITULO	PUESTO	CONTACTO	OTRO
18	Licenciatura	Derecho	6 https://www.triejal.gob.mx/pdf/CV/lumenet_solis_lose_zafael.pdf	No
19	Licenciatura	Derecho	6 https://www.triejal.gob.mx/pdf/CV/orozco_barajas_pedro_alfonso.pdf	No
20	Licenciatura	Derecho	6 https://www.triejal.gob.mx/pdf/CV/solis_peres_hector_fernando.pdf	No
21	Licenciatura	Derecho	6 https://www.triejal.gob.mx/pdf/CV/enriquez_ramirez_viviana.pdf	No
22	Licenciatura	Derecho	6 https://www.triejal.gob.mx/pdf/CV/peres_coato_david.pdf	No
23	Licenciatura	Derecho	6 https://www.triejal.gob.mx/pdf/CV/salcedo_artiaga_ricardo.pdf	No
24	Licenciatura	Derecho	6 https://www.triejal.gob.mx/pdf/CV/lopez_irmae_cv.pdf	No
25	Licenciatura	Derecho	6 https://www.triejal.gob.mx/pdf/CV/diaz_carlos_christian.pdf	No
26	Licenciatura	Derecho	6 https://www.triejal.gob.mx/pdf/CV/tello_gudino_luisa_cristina.pdf	No
27	Licenciatura	Derecho	6 https://www.triejal.gob.mx/pdf/CV/cervantes_lopez_edgar_rogerio.pdf	No
28	Licenciatura	Derecho	6 https://www.triejal.gob.mx/pdf/CV/trip_marias_manuel_de_levus.pdf	No
29	Maestría	Derecho	6 https://www.triejal.gob.mx/pdf/CV/ireti-sandovalCV.pdf	No
30	Licenciatura	Derecho	6 https://www.triejal.gob.mx/pdf/CV/lopez_jacobo_victor_hugo.pdf	No
31	Licenciatura	Derecho	6 https://www.triejal.gob.mx/pdf/CV/benjamin-sanchezCV.pdf	No
32	Maestría	Derecho	6 https://www.triejal.gob.mx/pdf/CV/miriam-rangelCV.pdf	No
33	Licenciatura	Derecho	6 https://www.triejal.gob.mx/pdf/CV/samuel-martinez.pdf	No
34	Licenciatura	Derecho	6 https://www.triejal.gob.mx/pdf/CV/quintero_olvera_ricardo_alejandro.pdf	No
35	Licenciatura	Derecho	7 https://www.triejal.gob.mx/pdf/CV/marquez_trujillo_beatriz_adriana.pdf	No
36	Licenciatura	Derecho	7 https://www.triejal.gob.mx/pdf/CV/hurtado_tinto_alejandro.pdf	No
37	Licenciatura	Derecho	7 https://www.triejal.gob.mx/pdf/CV/lopez_marcos_maria_de_los_angeles.pdf	No
38	Licenciatura	Derecho	8 https://www.triejal.gob.mx/pdf/CV/martinez_martinez_faviola_jacqueline.pdf	No
39	Licenciatura	Derecho	9 https://www.triejal.gob.mx/pdf/CV/arredondo_wilson_alejandra.pdf	No
40	Licenciatura	Derecho	10 https://www.triejal.gob.mx/pdf/CV/allieros_castro_laura.pdf	No
41	Licenciatura	Contador Público	10 https://www.triejal.gob.mx/pdf/CV/cortes_solares_margarita.pdf	No
42	Maestría	Derecho	10 https://www.triejal.gob.mx/pdf/CV/magalanes_escalera_cesar_octavio.pdf	No
43	Licenciatura	Derecho	10 https://www.triejal.gob.mx/pdf/CV/tronelli_fernando.pdf	No
44	Licenciatura	Derecho	10 https://www.triejal.gob.mx/pdf/CV/camarena_schmitz_antonio.pdf	No
45	Licenciatura	Derecho	10 https://www.triejal.gob.mx/pdf/CV/lopez_barreto_jose_manuel.pdf	No

En lo que respecta parte del cuestionamiento sí han tenido brechas de ciberseguridad desde el año 2015 a la fecha de la presente solicitud y señalar cuántas, ninguna en el plazo requerido.

Por lo que respecta al cuestionamiento de sí se han adoptado esquemas de mejores prácticas en materia de protección de datos personales. Le comunico que se desarrollaron los siguientes documentos:

1. Políticas Internas de Gestión y Tratamiento de Datos Personales del Tribunal Electoral del Estado de Jalisco.
2. Criterios Generales de Protección de Información Confidencial y Reservada del Tribunal Electoral del Estado de Jalisco.

Ahora bien, en lo que respecta parte del **cuestionamiento de 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**, hago de su conocimiento que en este momento no se cuenta con una plataforma informática activa o aplicación tecnológica que realice tratamiento a datos personales.

Así mismo, en lo que respecta al **cuestionamiento de sí se cuenta con documento de seguridad en materia de protección de datos personales**, se le comunica que la versión pública del documento de seguridad, puede consultarse y descargarse en el siguiente link correspondiente a la página oficial de este Sujeto Obligado:

[https://www.triejal.gob.mx/documento\\_de\\_seguridad/](https://www.triejal.gob.mx/documento_de_seguridad/)

Documento que atiende las siguientes acciones:

- MEDIDAS DE SEGURIDAD IMPLEMENTADAS
- CONTROLES Y MECANISMOS DE SEGURIDAD PARA LAS TRANSFERENCIAS
- BITÁCORAS DE ACCESO, OPERACIÓN COTIDIANA Y VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES
- CONTROLES DE IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS
- PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES
- TÉCNICAS DE SUPRESIÓN Y BORRADO SEGURO DATOS PERSONALES
- ANÁLISIS DE RIESGOS
- IDENTIFICACIÓN DE MEDIDAS DE SEGURIDAD
- GESTIÓN DE VULNERACIONES





- PLAN DE CONTINGENCIA PARA LA PROTECCIÓN DE LA INFORMACIÓN DEL TRIBUNAL ELECTORAL DEL ESTADO DE JALISCO
- MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD
- ANÁLISIS DE BRECHA
- PLAN DE TRABAJO
- PROGRAMA GENERAL DE CAPACITACIÓN
- CATÁLOGO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Por todo lo anterior y en virtud que del contenido del acuerdo y su anexo, se da contestación a lo peticionado, se tiene dando respuesta a la información requerida por la parte solicitante<sup>1</sup>. Asimismo, la información se entrega en el estado que se encuentra, sin que exista obligación de procesar, calcular o presentar la información de forma distinta a como se encuentre, lo anterior de acuerdo a lo establecido por el numeral 87, párrafo 3 de la multicitada Ley.

Por tal virtud, se determina que la información solicitada es **Información Pública Ordinaria**<sup>2</sup>, razón por la cual la respuesta de acceso es en sentido **AFIRMATIVO**.

**PRIMERO.** Se radicó la presente solicitud bajo el número de expediente **TEEJ-INFO-185/2024**, se determinó que la misma cumplió con los requisitos mínimos necesarios para su admisión a trámite.

**SEGUNDO.** En virtud del contenido de la resolución se tiene dando respuesta a la parte solicitante.

<sup>1</sup> De conformidad a lo dispuesto por el artículo 87, fracción IV, de la ley de la materia.

<sup>2</sup> Acorde al catálogo establecido por el artículo 8, párrafo 1, fracción IV, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.

**TERCERO.** Se determina que la información solicitada es Información Pública Ordinaria, razón por la cual la respuesta de acceso es en sentido afirmativo.

**Notifíquese** a la parte solicitante a través de la Plataforma Nacional de Transparencia.



Unidad de  
Transparencia y  
Protección de  
Datos Personales

**CÉSAR OCTAVIO MAGALLANES ESCALERA**  
**JEFE DE DEPARTAMENTO DE LA UNIDAD DE TRANSPARENCIA Y PROTECCIÓN**  
**DE DATOS PERSONALES DEL TRIBUNAL ELECTORAL DEL ESTADO DE**  
**JALISCO.**

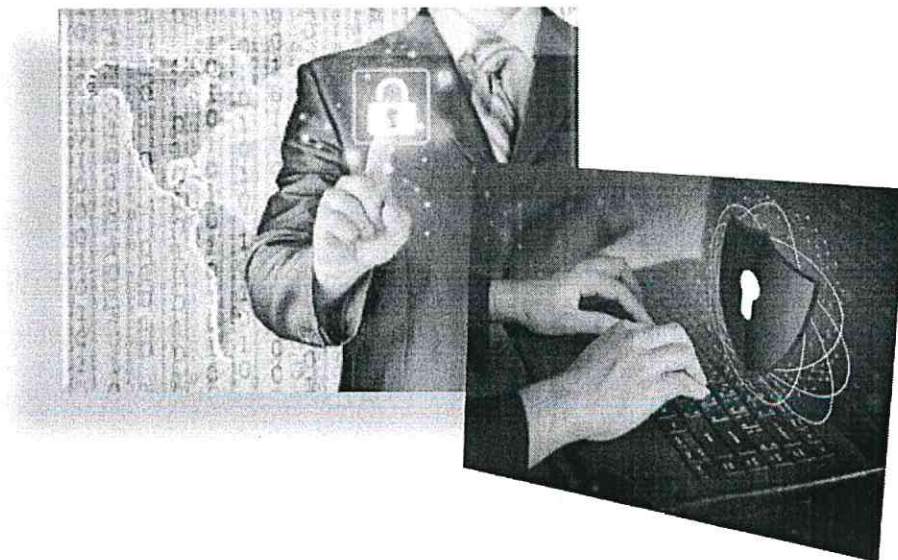




**TRIBUNAL**  
**ELECTORAL**  
DEL ESTADO DE JALISCO

# DOCUMENTO DE SEGURIDAD

TRIBUNAL ELECTORAL DEL ESTADO DE JALISCO



## INTRODUCCIÓN

En el Tribunal Electoral del Estado de Jalisco (TRIEJAL), la información es un activo que debe protegerse mediante un conjunto coherente de procesos y sistemas diseñados, administrados y mantenidos por este Órgano Jurisdiccional. De esta manera, la gestión de la seguridad de la información, como parte de un sistema administrativo más amplio, busca establecer, implementar, operar, monitorear y mejorar los procesos y sistemas relativos a la confidencialidad, integridad y disponibilidad de la información, aplicando un enfoque basado en los riesgos que la Institución afronta. El presente Documento de Seguridad para Sistemas de Datos Personales en medios físicos (Documento), se dicta en cumplimiento de las disposiciones jurídicas vigentes, con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen.

El Documento brinda al TRIEJAL homogeneidad en la organización, procesos y sistemas, en el que el Comité de Transparencia, conjuntamente con el área de Informática y los responsables de los sistemas de datos personales, definen las medidas de seguridad administrativa, física y tecnológicas implementadas para la protección de los sistemas de datos personales custodiados.

Así mismo, este documento tiene como propósito controlar internamente el universo de sistemas de datos personales que posee el TRIEJAL, el tipo de datos personales que contiene cada uno, los responsables, encargados, usuarios de cada sistema y las medidas de seguridad concretas implementadas.



## Documento de Seguridad

# CONTENIDO

INTRODUCCIÓN.....	1
GLOSARIO.....	3
MEDIDAS DE SEGURIDAD IMPLEMENTADAS.....	6
CONTROLES Y MECANISMOS DE SEGURIDAD PARA LAS TRANSFERENCIAS.....	7
BITÁCORAS DE ACCESO, OPERACIÓN COTIDIANA Y VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES.....	8
CONTROLES DE IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS.....	9
PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES.....	10
TÉCNICAS DE SUPRESIÓN Y BORRADO SEGURO DATOS PERSONALES.....	11
ANÁLISIS DE RIESGOS.....	12
IDENTIFICACIÓN DE MEDIDAS DE SEGURIDAD.....	13
GESTIÓN DE VULNERACIONES.....	20
PLAN DE CONTINGENCIA PARA LA PROTECCIÓN DE LA INFORMACIÓN DEL TRIBUNAL ELECTORAL DEL ESTADO DE JALISCO.....	20
MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD.....	28
ANÁLISIS DE BRECHA.....	31
PLAN DE TRABAJO.....	33
PROGRAMA GENERAL DE CAPACITACIÓN.....	36
CATÁLOGO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES.....	38
ANEXO 1.....	51
ANEXO 2.....	52
ANEXO 3.....	53



**TRIBUNAL  
ELECTORAL**  
DEL ESTADO DE JALISCO

## GLOSARIO

Bases de datos	Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionado a criterios determinados con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.
Disociación	El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo.
Documento de seguridad	Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.
Encargado	Persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras, trata datos personales a nombre y por cuenta del responsable.
Evaluación de impacto en la protección de datos personales	Documento mediante el cual se valoran y determinan los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar, prevenir y mitigar posibles riesgos que puedan comprometer el cumplimiento de los principios, deberes, derechos y demás obligaciones.
INAI	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.
Instituto	Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco.
LAN	Una red de área local o LAN (por las siglas en inglés



	de Local Area Network) es una red de computadoras que abarca un área reducida a una casa, un departamento o un edificio.
Ley	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.
Ley de Transparencia	Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.
Ley General	Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
Ley General de Transparencia	Ley General de Transparencia y Acceso a la Información Pública.
Medidas de seguridad	Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten garantizar la protección, confidencialidad, disponibilidad e integridad de los datos personales.
Medidas de seguridad administrativas	Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización, formación y capacitación del personal en materia de protección de datos personales.
Medidas de seguridad físicas	Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.
Medidas de seguridad técnicas	Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y recursos involucrados en su tratamiento.
N/A	No aplica.

Responsable	Los sujetos obligados señalados en el artículo 1, párrafo 5, de la presente Ley que determinarán los fines, medios y alcance y demás cuestiones relacionadas con un tratamiento de datos personales.
Supresión	La baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable.
Titular	Persona física a quien pertenecen los datos personales.
Transferencia	Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, responsable o encargado.
Tratamiento	De manera enunciativa más son limitativa cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.



## MEDIDAS DE SEGURIDAD IMPLEMENTADAS

### Medidas de seguridad físicas

La seguridad física consiste en la aplicación de barreras físicas, y procedimientos de control como medidas de prevención y contra medidas ante amenazas a los recursos y la información confidencial, se refiere a los controles y mecanismos de seguridad dentro y alrededor de la obligación física de los sistemas informáticos así como los medios de acceso remoto al y desde el mismo, implementados para proteger el hardware y medios de almacenamiento de datos.

#### Entorno Institucional

- 
- 
- ELIMINADO: seis elementos, Información Reservada
- Artículo 17.1, fracción I inciso a) LTAIPEJM. Medidas de
- Seguridad físicas. Su publicación pondría en riesgo al
- Tribunal y los Datos Personales que se protegen pues
- reflejaría las posibles vulnerabilidades.
- 

#### Entorno de los datos

- No se sitúan equipos en sitios altos para evitar caídas,
- No se colocan elementos móviles sobre los equipos para evitar que caigan sobre ellos,
- Se separan los equipos de las ventanas para evitar que caigan por ellas o qué objetos lanzados desde el exterior los dañen o sufran daño por lluvia
- Colocar los equipos sobre plataformas de goma para que esta absorba las vibraciones,
- El Tribunal está provisto de equipo para la extinción de incendios conforme a lo determinado por un proveedor externo certificado.
- El Tribunal Cuenta con detectores de humo en las áreas de archivo.

## CONTROLES Y MECANISMOS DE SEGURIDAD PARA LAS TRANSFERENCIAS

### **Transmisiones mediante el traslado de soportes físicos**

- a) El envío se realiza a través de personal de Oficialía de Partes a la Secretaría General de Acuerdos o mediante personal autorizado por su superior jerárquico mediante acuse sello y firma de recibido.
- b) Cuando se transfiere información confidencial esta se realiza en sobres
- c) La información sólo es entregada a los titulares de la información o sus autorizados, previa acreditación con identificación oficial
- d) Toda entrega de información requiere acuse de recibo, e identificación.
- e) A partir de la aprobación del presente documento todas las transmisiones serán registradas en las bitácoras de transferencia de cada área.

### **Transmisiones mediante el traslado físico de soportes electrónicos**

- a) El envío se realiza a través de personal de Oficialía de Partes a la Secretaría General de Acuerdos o mediante personal autorizado por su superior jerárquico mediante acuse sello y firma de recibido.
- b) Cuando se transfiere información confidencial esta se realiza en sobres sellados y se utiliza la leyenda de clasificación señalada en los Lineamientos Generales para Clasificación y Desclasificación de la Información, así como para la Elaboración de las Versiones Públicas.
- c) La información sólo es entregada a los titulares de la información o sus autorizados, previa acreditación con identificación oficial
- d) Toda entrega de información requiere acuse de recibo e identificación.
- e) A partir de la aprobación del presente documento todas las transmisiones serán registradas en las bitácoras de transferencia de cada área.



f) A partir de la aprobación del presente documento todos los soportes electrónicos que sean transferidos y contengan información confidencial deberán estar cifrados.

### **Transmisiones mediante el traslado sobre redes electrónicas**

A partir de la aprobación del presente documento todos los soportes electrónicos que sean transferidos y contengan información confidencial deberán ser sometidos a un proceso a través del cual la información puede ser codificada para no ser accedida por otros, a menos que tengan la clave del cifrado.

### **Tipos de Transferencias:**

Internos e interinstitucionales

### **Tipo de traslado:**

De soportes físicos, físico de soportes electrónicos, sobre redes electrónicas

## **BITÁCORAS DE ACCESO, OPERACIÓN COTIDIANA Y VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES**

### **Seguridad de los Datos Personales**

#### **Bitácoras de Acceso**

1. Las bitácoras de acceso a los datos personales se utilizan en los soportes

Físicos y contienen la siguiente información:

- a) Nombre y cargo de quien accede
- b) Identificación del Expediente



**TRIBUNAL  
ELECTORAL**  
DEL ESTADO DE JALISCO

- c) Fojas del Expediente
  - d) Propósito del Acceso
  - e) Fecha de Acceso
  - f) Hora de Acceso
  - g) Fecha de Devolución
  - h) Hora de Devolución
2. **ELIMINADO:** dos renglones, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Medidas de Seguridad y ubicación de las bitácoras. Su publicación pondría en riesgo al Tribunal pues indicaría la ubicación de las bitácoras y su posible alteración.

### **Vulneraciones a la Seguridad de los Datos Personales**

La bitácora de vulneraciones contiene la siguiente información

1. Nombre de quien reporta el incidente
2. Cargo
3. La fecha en la que ocurrió;
4. El motivo de la vulneración de seguridad; y
5. Las acciones correctivas implementadas de forma inmediata y definitiva.

## **CONTROLES DE IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS**

Las vulnerabilidades pueden darse a la hora de identificar sus usuarios y los permisos que estos poseen por lo que debe evitarse los riesgos de producirse situaciones como el escalado de privilegios o la suplantación de identidad.

Hay dos procesos distintos que intervienen cuando se trata de permitir a un usuario acceder

La autenticación es el proceso de identificación de un individuo sobre la base de sus credenciales (normalmente nombre de usuario y contraseña).

El control de acceso es el proceso de decidir si el usuario tiene permiso para ejecutar algo o no. También llamado autorización, se refiere a la gestión del



acceso a los recursos protegidos y al proceso de determinar si un usuario está autorizado a acceder a un recurso particular. Por ejemplo, hay recursos que sólo están disponibles para los usuarios autenticados, recursos que sólo están disponibles para los administradores, y los recursos que están disponibles para todos. Así, al establecer privilegios de acceso a los usuarios podemos asegurar la confidencialidad y disponibilidad de la información.

#### Identificación

- ELIMINADO: 3 elementos, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Controles de identificación y autenticación. Su publicación pondría en riesgo al Tribunal pues reflejaría las posibles vulnerabilidades.
- 

#### Acceso

- ELIMINADO: 2 elementos, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Controles de identificación y acceso. Su publicación pondría en riesgo al Tribunal pues reflejaría las posibles vulnerabilidades.
- 

## PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES

**Objeto:** Garantizar la seguridad de la información mediante la realización de copias de respaldo y su recuperación cuando sea requerido.

**Alcance:** Realizar el respaldo de información del Tribunal en los equipos que contengan bases de datos y asegurar el resguardo y custodia de los medios de respaldo que se generen.

**Respaldo:** Cada área será la responsable de almacenar sus respaldos durante el tiempo que señale el catálogo de disposición documental del Tribunal, atendiendo, a las recomendaciones de la Unidad de Transparencia, así como del Oficial de Protección de Datos Personales.

Los respaldos se almacenan en discos duros o discos magnéticos.

Los responsables de cada área deben Identificar claramente la información crítica que se debe respaldar, indicando los niveles de seguridad e incluir las condiciones necesarias para futuras restauraciones.

Las cintas de respaldo se deberán identificar con el contenido y fecha de realización.

Establecer por área de acuerdo a sus necesidades la frecuencia y tipo de respaldo ya sea parcial, completo, incremental, mensual, semanal, o diario.

**Recuperación:** Los respaldos contienen fecha y hora, tanto inicial como final. La recuperación se realiza cruzando la fecha del incidente y el último respaldo.

El responsable de las copias de seguridad debe realizar trimestralmente pruebas de recuperación y calidad de la información de manera aleatoria, y dejar de dicha prueba.

## TÉCNICAS DE SUPRESIÓN Y BORRADO SEGURO DATOS PERSONALES

### MÉTODOS FÍSICOS

- Trituración mediante corte cruzado o en partículas: Cortar el documento de forma vertical y horizontal generando fragmentos diminutos, denominados "partículas", lo cual hace prácticamente imposible que se puedan unir.
- Destrucción de los medios de almacenamiento electrónicos mediante desintegración, consistente en separación completa o



pérdida de la unión de los elementos que conforman algo, de modo que deje de existir.

## MÉTODOS LÓGICOS

- Sobre-escritura: consiste en sobrescribir todas las ubicaciones de almacenamiento utilizables en un medio de almacenamiento, es decir, se trata de escribir información nueva en la superficie de almacenamiento, en el mismo lugar que los datos existentes, utilizando herramientas de software.

## ANÁLISIS DE RIESGOS

ELIMINADO: Un párrafo. Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Análisis de riesgos de los datos en posesión del Tribunal, puede poner en riesgo a los datos personales por la divulgación del mismo.

ELIMINADO: Un párrafo. Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Análisis de riesgos de los datos en posesión del Tribunal, puede poner en riesgo a los datos personales por la divulgación del mismo.

ELIMINADO: Un párrafo. Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Análisis de riesgos de los datos en posesión del Tribunal, puede poner en riesgo a los datos personales por la divulgación del mismo.



ELIMINADO: Una tabla. Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Análisis de riesgos de los datos en posesión del Tribunal, puede poner en riesgo a los datos personales por la divulgación del mismo.

## IDENTIFICACIÓN DE MEDIDAS DE SEGURIDAD

<b>Medidas de Seguridad Administrativas</b>	<p>ELIMINADO. Una tabla. Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Condiciones de los datos en posesión del Tribunal, puede poner en riesgo a los datos personales por la divulgación del mismo.</p>
---	---





**TRIBUNAL  
ELECTORAL**  
DEL ESTADO DE JALISCO

ELIMINADO. Una tabla. Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Condiciones de los datos en posesión del Tribunal, puede poner en riesgo a los datos personales por la divulgación del mismo.



ELIMINADO. Una tabla. Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Condiciones de los datos en posesión del Tribunal, puede poner en riesgo a los datos personales por la divulgación del mismo.





**TRIBUNAL  
ELECTORAL**  
DEL ESTADO DE JALISCO

Documento de Seguridad para la Protección de Datos  
Personales del Tribunal Electoral del Estado de Jalisco.

	Control	Parámetro
<p><b>Medidas de Seguridad Avanzadas para Accesos desde Red Interna RI-3 conforme a la metodología BAA del INAI</b></p>		<p>ELIMINADO. Una tabla. Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Condiciones de los datos en posesión del Tribunal, puede poner en riesgo a los datos personales por la divulgación del mismo.</p>





**TRIBUNAL  
ELECTORAL**  
DEL ESTADO DE JALISCO

	<p>ELIMINADO. Una tabla. Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Condiciones de los datos en posesión del Tribunal, puede poner en riesgo a los datos personales por la divulgación del mismo.</p>	
<b>Medidas de Seguridad Físicas</b>	<b>Control</b>	<b>Parámetro</b>
	<p>ELIMINADO. Una tabla. Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Condiciones de los datos en posesión del Tribunal, puede poner en riesgo a los datos personales por la divulgación del mismo.</p>	





**TRIBUNAL  
ELECTORAL**  
DEL ESTADO DE JALISCO

	ELIMINADO. Una tabla. Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Condiciones de los datos en posesión del Tribunal, puede poner en riesgo a los datos personales por la divulgación del mismo.	
Medidas Reforzadas de Seguridad para Accesos desde Entornos de Alta Anonimidad	Control	Parámetro
	ELIMINADO. Una tabla. Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Condiciones de los datos en posesión del Tribunal, puede poner en riesgo a los datos personales por la divulgación del mismo.	



ELIMINADO. Una tabla. Información Reservada Artículo 17.1  
fracción I inciso a) LTAIPEJM. Condiciones de los datos en  
posesión del Tribunal, puede poner en riesgo a los datos  
personales por la divulgación del mismo.



## GESTIÓN DE VULNERACIONES

### Plan de respuesta

- 1) Restauración Inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos.
- 2) En caso de que la vulneración fuera resultado de la comisión de un delito realizar las denuncias correspondientes.
- 3) Llenado de Formato A (anexo 1), por parte de la persona que detectó la vulneración.
- 4) Llenado de Formato B (anexo 2), por parte de la Unidad de Transparencia y Protección de Datos Personales.
- 5) Determinación de la magnitud de la afectación y elaboración de recomendaciones para los titulares.
- 6) Elaboración de Informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Unidad de Transparencia.
- 7) Notificación a titulares en un lapso de 72 horas que de forma significativa vean afectados sus derechos patrimoniales o morales.
- 8) Llenado de la bitácora de vulneraciones conforme al artículo 39 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y Municipios.

## PLAN DE CONTINGENCIA PARA LA PROTECCIÓN DE LA INFORMACIÓN DEL TRIBUNAL ELECTORAL DEL ESTADO DE JALISCO.

### Clasificación de la contingencia:

Grado de afectación según sea el tipo de la contingencia:



**TRIBUNAL  
ELECTORAL**  
DEL ESTADO DE JALISCO

**Grado 1:** Pueden ser resueltas por el mismo personal del Tribunal; van desde fallas eléctricas, fallas con la conexión de internet.

**Grado 2:** Requiere la colaboración de personal del Tribunal y personal externo, verbigracia en un incendio apoyo del cuerpo de bomberos y protección civil.

**Grado 3:** Por sus alcances pueden afectar severamente la operatividad del Tribunal y se requiere además del apoyo externo.

### **Consideraciones Principales**

- Se debe realizar una evaluación de los riesgos.
- Dentro de la implementación del plan de contingencia se debe contar con un responsable general quien guiará la implementación del mismo, así como la toma de las decisiones.
- Se designe a un encargado de cada área para que apoye en cualquier desastre que ocurra y genere la contingencia, capacitándolos para el manejo de las mismas, como el uso de extintores, planes de evacuación etc.
- Es necesario hacer las pruebas previas del plan de contingencia para garantizar su funcionalidad en caso de siniestro (las pruebas generalmente se hacen en tiempo real y lo más aproximados a la realidad).
- Reunión con las comisiones o brigadas de las áreas de la Municipalidad (capacitación y evaluaciones)
- Revisión del Plan e integración de las recomendaciones y decisiones adoptadas de acuerdo con las lecciones aprendidas del ejercicio.
- Difusión del documento del plan de contingencia una vez aprobado.

### **Lugar alternativo de trabajo**

En caso de algún desastre mayor (terremoto o incendio) que implique pérdidas estructurales se plantea en algunos casos la posibilidad de contar con algún lugar alternativo de trabajo los sitios alternos de trabajo pueden ser: propios de la organización, de una entidad con la que hay acuerdo o reciprocidad, instalaciones alquiladas (se debe contar con presupuesto).

**En caso de contar con un ambiente alterno debe contar con los siguientes recursos:**



- Mesas para monitores y teclados de los servidores principales
- Sillas
- Switches
- Router para la conexión a internet
- UPS
- Teléfono
- Extinguidor
- Útiles de Oficina

### **Medidas preventivas ante siniestros**

#### **Medidas de prevención y conservación de los archivos:**

- El archivo general debe situarse en el primer piso del edificio (no sótanos).
- Espacios con luz natural y sin humedad.
- Los muebles de archivo deben garantizar la conservación de los documentos que guardan; los documentos deben guardar uniformidad.
- Evitar archivar documentación cerca de aparatos eléctricos, las instalaciones eléctricas deben estar en buenas condiciones.
- Los estantes de los archivos deben de estar entre 10 y 15 cm del suelo (facilitan la limpieza y evita su vez la acumulación de humedad y proliferación de plagas)
- Todos los equipos eléctricos que estén en el archivo deben quedar apagados y desconectados durante la noche o cuando no se utilicen.
- Se recomienda no colocar vasos con líquido que puedan derramarse fácilmente sobre los aparatos eléctricos.

### **Incendios**

#### **Medidas preventivas en caso de Incendios**

- ❖ Se recomienda tener un conocimiento básico de primeros auxilios.
- ❖ Para la pronta detección de un incendio se puede contar con detectores de humo.

- ❖ En caso de incendio no abrir puertas y ventanas, el aire es factor para propagación del fuego.
- ❖ Si se tienen almacenadas sustancias inflamables como gasolina, acetona, aguarrás, alcohol o tiner, se sugiere colocarlos en lugares ventilados y lejos de las flamas, fuentes de calor y aparatos eléctricos (si no los necesita, deséchelos preferentemente)
- ❖ Si el incendio es pequeño, se procurará apagarlo mediante un extintor. Si el fuego es de origen eléctrico no se deberá intentar apagarlo con agua.
- ❖ No sobrecargar los contactos eléctricos, desconectando los que no se utilicen.

### **Sobre el resguardo de la información en caso de incendio:**

- ❖ Respaldo de información en una zona segura de preferencia, donde el calor de un incendio no alcance los dispositivos, esto es en lugares cercanos a los extintores (sugerencias para realizar el almacenamiento de la información: CD, Disco duro, bases de datos, la nube únicamente si es segura).
- ❖ Tener identificados los documentos con mayor valor para resguardarlos en una zona segura (como en una caja de seguridad o realizar la digitalización de los mismos con resguardo en la nube).

### **Durante un incendio:**

- Ubicar los extintores cerciórese de saber usarlos y que estos sean utilizables.
- Si detecta un incendio procure mantener la calma y repórtelo inmediatamente o presione alguna señal de alarma.
- No abra puertas ni ventanas el fuego se extiende con el aire.
- Si es un incendio que no puede controlar usted mismo llame a los bomberos.
- No pierda tiempo buscando objetos personales y salga del inmueble lo antes posible.
- Si hay gas o humo humedezca un trapo y cubra su nariz y boca.
- Si existe una puerta que deba atravesar toque con precaución la perilla; si está caliente no la abra.
- Si su ropa se enciende; tírese al piso y ruede lentamente.

### **Después del Incendio:**



Un técnico debe de revisar las instalaciones de gas y electricidad antes de utilizarlas nuevamente.

## Terremoto

El daño ocasionado por un terremoto puede dañar principalmente la estructura del edificio, sin embargo si los datos almacenados se encuentran en discos duros, cd, USB, al contar con un respaldo de información incluso en la nube se tiene un respaldo inmediato, que permitiría recuperar la información si los otros respaldos físicos se dañaran, para inmediatamente apenas se tenga una conexión a internet y una computadora tener acceso a dichos respaldos.

## Medidas preventivas en caso de sismo

- No colocar muebles, equipos o cajas que bloqueen las rutas y salidas de emergencia del archivo.
- Contar con un teléfono celular de emergencia en caso de falla de líneas telefónicas fijas.
- Contar con un plan de evacuación y realizar simulacros de manera cotidiana.
- Tener a la mano una radio de baterías, linterna y los principales documentos personales.
- Contar con un botiquín de primeros auxilios.
- Si se tienen anaqueles, los objetos pesados se colocan al final.
- Localizar los lugares seguros en cada cuarto; bajo mesas sólidas y escritorios resistentes
- Ubicar los lugares peligrosos: como ventanas donde los vidrios pueden estrellarse, libreros o muebles que podrían caerse en caso de sismo.

## Durante un sismo

- Mantener la calma y ubicar en una zona de segura.
- Pararse bajo un marco de puerta con trabe o de espaldas a un muro de carga.
- Adoptar posición fetal de cara al suelo, abrazándose usted mismo en un rincón, de ser posible protegerse la cabeza.
- Alejarse de ventanas, espejos y objetos de vidrio así como de objetos colgantes.
- Retirarse de objetos calientes, libreros, gabinetes, o muebles pesados.

- Si se está en un edificio evitar el uso de elevadores, si se está en la calle evitar los postes, árboles, ramas y balcones.
- Si es posible cerrar llaves del gas, desconecte la alimentación eléctrica y no encender fuego.

### **Después de un Sismo:**

- Si usted quedo atrapado, conserve la calma y trate de comunicarse al exterior golpeando un objeto.
- Evite pisar cables que hubieran quedado caídos o sueltos.
- Encienda la radio para mantenerse informado (posibles replicas).
- En caso de visible daño estructural del edificio debe ser evaluado por protección civil para evitar cualquier riesgo secundario.
- Se deben revisar las instalaciones eléctricas y de gas principalmente para evitar un desastre secundario.

### **Inundaciones por lluvia**

#### **Medidas preventivas en caso de inundación**

- Es importante realizar la revisión y reparación de la hermeticidad de ventanas y puertas, por donde podría filtrarse el agua de lluvia, así como impermeabilizar los techos en temporada de lluvias esto para evitar goteras.
- Evitar en lo posible colocar expedientes y/o documentos directamente sobre el piso.
- Respetar, al menos, una altura de 10 a 15 cm de los archiveros.
- Colocar barreras para el agua (cubrir los documentos con plásticos, cubetas o recipientes para las goteras) en la parte superior de los estantes dentro del local de archivo.
- Evacuar los documentos afectados hacia áreas ventiladas.
- Inmediatamente colocar papel secante en cada hoja de los expedientes.
- Si un documento se moja en su totalidad se puede realizar la congelación del mismo para su recuperación, debe realizarlo preferentemente un especialista (restauración).

#### **Durante una inundación**

- Desconectar servicios de luz, gas y agua.
- Mantenerse alejados de árboles y postes de luz.



- Evitar tocar o pisar cables eléctricos.
- Cubrir con bolsas de plástico aparatos u objetos que puedan dañarse con el agua.

### **Después de la inundación**

- Se puede expulsar el agua con una bomba de achique con motor de combustión o eléctrico, si hay suministro eléctrico garantizado en caso de emergencia, y si no hubiere, mediante esponjas, baldes, recogedores, etc.
- Cerciorarse de que los aparatos eléctricos estén secos antes de utilizarlos nuevamente
- Desinfectar las áreas afectadas pisos, muros y mobiliario rescatable, con agua, jabón y cloro para evitar enfermedades.
- Ventilar las áreas afectadas después de la inundación.

**Si los documentos han sufrido daños y se encuentran mojados, se debe seguir el procedimiento de congelación para recuperarlos. A continuación se describe este procedimiento para recuperar los documentos humedecidos:**

1. Se introduce la obra en una bolsa de polietileno con cierre de cremallera o termosellable. Es muy importante envolver el libro en plástico y reducir el volumen de aire para evitar la formación de condensación. Para que la congelación se realice de forma correcta, se debe dejar un amplio espacio entre los libros.
2. La cámara de congelación debe alcanzar una temperatura de  $-20^{\circ}\text{C}$ . En un proceso acelerado de descenso de la temperatura el tratamiento será más efectivo. La temperatura debe ser constante y el congelador no ha de formar hielo ya que se puede acumular humedad. Se recomienda que en el momento de Aplicación combinada de los tratamientos de congelación y vacío para la desinfección de documentos. Se debe Depositar la obra en la cámara de congelación hasta que esta haya alcanzado dicha temperatura, para evitar la aclimatación de los organismos.
3. El tratamiento debe durar como mínimo 72 horas, dependiendo del grosor de la obra y la temperatura del congelador. No obstante, si es necesario, se puede alargar hasta un periodo de tres semanas.
4. La obra se ha de descongelar de forma paulatina sin ser extraída del envoltorio, hasta alcanzar el equilibrio con la temperatura ambiente. Una vez descongelada y alcanzado el equilibrio, el envoltorio se puede retirar.

### **Robo**



### **Robo Común de equipos:**

- o En caso de robo a mano armada se sugiere contar con teléfonos de emergencia de diferentes dependencias, así como un botón de pánico por medio de una App instalada en el celular. (<https://fge.jalisco.gob.mx/content/boton-de-panico>)

### **Huelga o Manifestaciones**

#### **Manifestación o huelga:**

- Si el archivo tiene cerradura, asegúrese que quede bajo llave.

### **Amenazas informáticas**

#### **Medidas preventivas para amenazas informáticas**

**Es necesario contar con un inventario actualizado de los equipos de cómputo, impresoras, escáner, fotocopadoras etc., y tener contacto con proveedores de software, hardware, y medios de soporte.**

- Prevención de falla de los equipos: se debe procurar dar mantenimiento preventivo por lo menos dos veces al año, y contar con proveedores en caso de que se requiera algún remplazo inmediato.
- Los equipos pueden quedar dañados por fallas eléctricas, se requiere contar con estabilizadores /reguladores, en cada uno de los equipos principalmente en aquellos que su afectación implique la pérdida de información importante.

### **Hackeo informático:**

Ante un evento de hackeo informático los pasos a seguir para mantener la seguridad de la información, son los siguientes:

#### **Cambiar contraseñas.**

- Debe tener al menos ocho caracteres
- No debe contener información personal como nombre real, nombre de usuario o incluso el nombre del Instituto
- Debe ser muy distinta a tus contraseñas previas
- No debe contener palabras completas
- Debe contener caracteres de las cuatro categorías primarias: mayúsculas, minúsculas, números y caracteres especiales



Mientras se está conectado a Internet el Hacker tendrá acceso a los archivos e información guardados en la computadora hackeada. Por lo que se debe desconectar el cable de la red lo antes posible.

Posteriormente:

- Contactar al personal de soporte para que retire del aire la página.
- Evalúe los daños causados: El experto debe evaluar qué información se perdió y cuál es la que se mantiene para restaurar el sitio lo antes posible. Mantener la misma dirección web Cuando la página fue atacada la dirección usualmente no se ve afectada. Lo que generalmente se pierde es la información (textos, videos, fotos, audios) que contenía. Se sugiere restaurar el sitio con la misma dirección, para que los usuarios no se confundan.

Referencias:

[http://www.itei.org.mx/v3/documentos/art8-13/documento\\_de\\_seguridad\\_itei\\_version\\_publica.pdf](http://www.itei.org.mx/v3/documentos/art8-13/documento_de_seguridad_itei_version_publica.pdf)

## **MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD**

En el Tribunal Electoral del Estado de Jalisco, tal y como lo establece el artículo 36 fracción XVIII de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, en el cual señala que se deben de contar con mecanismos de monitoreo y revisión de las medidas de seguridad, para auditar que en las distintas áreas del Tribunal efectúen de manera adecuada las directrices del Documento de Seguridad de la Protección de Datos Personales del Tribunal.

Dicha actividad se realizará con una temporalidad de 6 seis meses o en su caso de manera anticipada, cuando una medida de seguridad se vea vulnerada, siendo así, necesario la intervención de una auditoria en primer término de forma interna, externa siempre y cuando exista el presupuesto para ello o tal como lo establece el artículo 113 de la Ley de Protección de Datos Personales en Posesión



**TRIBUNAL  
ELECTORAL**  
DEL ESTADO DE JALISCO

de Sujetos Obligados del Estado de Jalisco y sus Municipios, por parte del Órgano Garante.

	Sí	No
1. Se han definido y se establecen y mantienen las medidas de seguridad administrativas, técnicas y físicas necesarias para la protección de los datos personales.	<input type="checkbox"/>	<input type="checkbox"/>
2. Se ha revisado el marco normativo que regula en lo particular el tratamiento de datos personales en cuestión, a fin de identificar si éste contempla medidas de seguridad, específicas o adicionales a las previstas en la LPDPPSOEJM y los Lineamientos Generales, y se ha definido la procedencia de su implementación.	<input type="checkbox"/>	<input type="checkbox"/>
3. El Programa de Protección de Datos Personales de la organización toma en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, e incluye lo siguiente: <ul style="list-style-type: none"><li>• El cumplimiento de todos los principios, deberes, derechos y demás obligaciones en la materia, de conformidad con lo previsto en la LPDPPSOEJM;</li><li>• Los roles y responsabilidades específicas de los involucrados internos y externos dentro de su organización, relacionados con los tratamientos de datos personales que se efectúen;</li><li>• Las sanciones en caso de incumplimiento;</li><li>• La identificación del ciclo de vida de los datos personales respecto de cada tratamiento que se efectúe; considerando la obtención, almacenamiento, uso, procesamiento, divulgación, retención, destrucción o cualquier otra operación realizada durante dicho ciclo en función de las finalidades para las que fueron recabados;</li><li>• El proceso general para el establecimiento, actualización, monitoreo y revisión de los mecanismos y medidas de seguridad; considerando el análisis de riesgo realizado previamente al tratamiento de los datos personales, y El proceso general de atención de los derechos ARCO.</li></ul>	<input type="checkbox"/>	<input type="checkbox"/>
3. Se han definido las funciones, obligaciones y cadena de mando de cada servidor público que trata datos personales, por unidad administrativa.	<input type="checkbox"/>	<input type="checkbox"/>
4. Se ha comunicado a cada servidor público sus funciones, obligaciones y cadena de mando con relación al tratamiento de datos personales que efectúa.	<input type="checkbox"/>	<input type="checkbox"/>
5. Se ha elaborado el inventario de datos personales con los siguientes elementos: <ul style="list-style-type: none"><li>• El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales;</li><li>• Las finalidades de cada tratamiento de datos personales;</li><li>• El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no;</li><li>• El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales;</li><li>• La lista de servidores públicos que tienen acceso a los sistemas de tratamiento;</li></ul>	<input type="checkbox"/>	<input type="checkbox"/>





**TRIBUNAL  
ELECTORAL**  
DEL ESTADO DE JALISCO

<ul style="list-style-type: none"><li>• En su caso, el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable, y</li><li>• En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que las justifican.</li></ul>		
<p>6. En el inventario de datos personales se tomó en cuenta el ciclo de vida de los datos personales, conforme a lo siguiente:</p> <ul style="list-style-type: none"><li>• La obtención de los datos personales;</li><li>• El almacenamiento de los datos personales;</li><li>• El uso de los datos personales conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin;</li><li>• La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen;</li><li>• El bloqueo de los datos personales, en su caso, y</li><li>• La cancelación, supresión o destrucción de los datos personales.</li></ul>	<input type="checkbox"/>	<input type="checkbox"/>
<p>7. Se ha realizado el análisis de riesgo, considerando lo siguiente:</p> <ul style="list-style-type: none"><li>• Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico;</li><li>• El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida;</li><li>• El valor y exposición de los activos involucrados en el tratamiento de los datos personales;</li><li>• Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida;</li><li>• El riesgo inherente a los datos personales tratados, contemplando el ciclo de vida de los datos personales, las amenazas y vulnerabilidades existentes para los datos personales y los recursos o activos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal o cualquier otro recurso humano o material, entre otros;</li><li>• La sensibilidad de los datos personales tratados;</li><li>• El desarrollo tecnológico;</li><li>• Las transferencias de datos personales que se realicen;</li><li>• El número de titulares;</li><li>• Las vulneraciones previas ocurridas en los sistemas de tratamiento, y</li><li>• El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.</li></ul>	<input type="checkbox"/>	<input type="checkbox"/>
<p>8. Se ha realizado el análisis de brecha, tomando en cuenta lo siguiente:</p> <ul style="list-style-type: none"><li>• Las medidas de seguridad existentes y efectivas;</li><li>• Las medidas de seguridad faltantes, y</li><li>• La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.</li></ul>	<input type="checkbox"/>	<input type="checkbox"/>

9. Se ha elaborado el plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales, a partir del análisis de riesgo y brecha realizado, y priorizando las medidas de seguridad más relevantes e inmediatas a establecer.	<input type="checkbox"/>	<input type="checkbox"/>
10. Se monitorea y revisa de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, tomando en cuenta lo siguiente: <ul style="list-style-type: none"> <li>• Los nuevos activos que se incluyan en la gestión de riesgos;</li> <li>• Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras;</li> <li>• Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;</li> <li>• La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;</li> <li>• Las vulnerabilidades identificadas para determinar aquellas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;</li> <li>• El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y</li> <li>• Los incidentes y vulneraciones de seguridad ocurridas.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>
11. Se cuenta con un programa de capacitación para los servidores públicos y externos involucrados en el tratamiento de datos personales, y se implementa.	<input type="checkbox"/>	<input type="checkbox"/>
12. Se implementa un sistema de gestión para la seguridad de los datos personales.	<input type="checkbox"/>	<input type="checkbox"/>
13. Se cuenta con el documento de seguridad con la información que establece el artículo 36 de la LPDPPSOEJM.	<input type="checkbox"/>	<input type="checkbox"/>
14. En el documento de seguridad se establece un procedimiento para su actualización, en caso de que ocurra alguno de los supuestos del artículo 36 de la LPDPPSOEJM.	<input type="checkbox"/>	<input type="checkbox"/>

## ANÁLISIS DE BRECHA

Medidas de seguridad faltantes por implementar por el Tribunal Electoral, (Metodología BAA, INAI).



**Medidas Reforzadas de Seguridad para Accesos desde Entornos de Alta Anonimidad:**

CONTROL	PARÁMETRO
ELIMINADO: Tabla. Información reservada artículo 17.1 fracción I inciso a) de la LTAIPEJM. Medidas de seguridad faltantes. Su publicación pondría en riesgo la información sensible en posesión del Tribunal pues reflejaría las posibles vulnerabilidades.	

**Medidas de Seguridad Avanzadas para Accesos desde Red Interna:**

CONTROL	PARÁMETRO
ELIMINADO: Tabla. Información reservada artículo 17.1 fracción I inciso a) de la LTAIPEJM. Medidas de seguridad faltantes. Su publicación pondría en riesgo la información sensible en posesión del Tribunal pues reflejaría las posibles vulnerabilidades.	

**Medidas de Seguridad Administrativas:**

CONTROL	PARÁMETRO
ELIMINADO: Tabla. Información reservada artículo 17.1 fracción I inciso a) de la LTAIPEJM. Medidas de seguridad faltantes. Su publicación pondría en riesgo la información sensible en posesión del Tribunal pues reflejaría las posibles vulnerabilidades.	



### Medidas de Seguridad Física:

CONTROL	PARÁMETRO
ELIMINADO: Tabla. Información reservada artículo 17.1 fracción I inciso a) de la LTAIPEJM. Medidas de seguridad faltantes. Su publicación pondría en riesgo la información sensible en posesión del Tribunal pues reflejaría las posibles vulnerabilidades.	

## PLAN DE TRABAJO

En este sentido, las medidas de seguridad físicas y técnicas que requieran la erogación de recursos como la compra de muebles incombustibles, y cestos metálicos para papeles y sustitución de los materiales plásticos e inflamables, se realizarán conforme a los tiempos administrativos del Tribunal y el presupuesto lo permita, y por lo que ve, a la capacitación del personal Jurídico Administrativo de este Tribunal Electoral, respecto al Tratamiento de Datos Personales será mediante tres cursos que se solicitaran al Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco y además asesoramiento y capacitación constante por parte de la Unidad de Transparencia y Protección de Datos Personales de este Tribunal Electoral.



➤ **PRIMERA ETAPA 1 A 6 MESES**

- Capacitación del personal Jurídico Administrativo de este Sujeto Obligado referente a "**Generalidades de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados**" impartido por personal del Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco.
- Disociación de información cuando los datos pasen de un ambiente de riesgo menor a un ambiente de riesgo mayor;
- Fuga de información: Se deben prevenir las oportunidades de fuga de información;
- Política sobre el uso de controles criptográficos: Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada.

➤ **SEGUNDA ETAPA 7 A 12 MESES**

- Capacitación del personal Jurídico Administrativo de este Sujeto Obligado referente a "**Principios y Deberes de Protección de Datos Personales en Posesión de Sujetos Obligados**". impartido por personal del Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco.
- Términos y condiciones de empleo: Como parte de su obligación contractual, los empleados, contratistas y usuarios de terceras partes, deben acordar y firmar los términos y condiciones de su contrato de empleo, el cual debe indicar su responsabilidad respecto a seguridad de la información.
- Administración de medios removibles: Deberán documentarse e implementarse procedimientos para la gestión de medios removibles.

- Acuerdos de intercambio de información: Deberán establecerse acuerdos para el intercambio de información y aplicaciones entre la organización y entidades externas
- Uso Sistema de monitoreo: Se deben establecer procedimientos para monitorear el uso de la información y los sistemas. Los resultados de las actividades de monitoreo deben ser revisados con regularidad.
- Verificación del cumplimiento técnico: Se deben verificar constantemente los sistemas de información para el cumplimiento de los estándares de seguridad.
- Distribución de las responsabilidades de seguridad de la información: Todas las responsabilidades de seguridad deben estar claramente definidas.

### ➤ TERCERA ETAPA 13 A 18 MESES

- Capacitación del personal Jurídico Administrativo de este Sujeto Obligado referente a "**Sistema de Gestión, Medidas de seguridad y acciones preventivas de Protección de Datos Personales en Posesión de Sujetos Obligados**". impartido por personal del Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco.
- Eliminación de los derechos de acceso: Los derechos de acceso de todos los empleados, contratistas y usuarios de terceras partes, a información e instalaciones de procesamiento de información deben ser removidos en cuanto se termine el trabajo, contrato, acuerdo o cuando se requiera hacer un ajuste.
- Eliminación y entrega de los medios de almacenamiento: Los medios deberán eliminarse de modo seguro cuando no se les necesite más, usando procedimientos formales.



## PROGRAMA GENERAL DE CAPACITACIÓN

Establecer un programa para capacitar al personal del sujeto obligado sobre el tema de protección de datos personales. Indicar la temporalidad de la capacitación, las áreas a capacitar, las sesiones y los temas.

### PRESENTACIÓN

En la actualidad es de suma importancia contar con los medios y mecanismos para abonar al fortalecimiento de la Cultura de Protección de Datos Personales, en el Estado de Jalisco, a través del decreto 26420/LX/17 el Congreso del Estado de Jalisco, se expide la LEY DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DEL ESTADO DE JALISCO Y SUS MUNICIPIOS, en la que establece en el Título Segundo, los Principios y Deberes, en particular en su artículo 36 fracción XIX, que nos refiere que el sujeto obligado debe de contar con un Programa General de Capacitación para los servidores públicos en los Sujetos Obligados. Por lo anterior, es pertinente y necesario actualizar y capacitar a los servidores públicos del Tribunal Electoral del Estado de Jalisco. Así pues, considerando las dinámicas y necesidades de las distintas áreas, la Unidad de Transparencia y Protección de Datos, pone a disposición el Programa General de capacitación, con la finalidad de dotar a la mayor parte de servidores públicos de la información actualizada, en materia de Protección de Datos Personales.

### OBJETIVO

Contribuir al fortalecimiento de la Cultura de Protección de Datos Personales, entre los servidores públicos del Tribunal Electoral del Estado de Jalisco, mediante la implementación de un Programa General de Capacitación, con la finalidad de mejorar la calidad y efficientar el cumplimiento de las disposiciones en la materia, tal como lo establece el artículo 91 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios

### TEMPORALIDAD

Las fechas para la implementación de las capacitaciones serán cada 4 cuatro meses, mismas que serán establecidas en base a la carga de trabajo de las distintas áreas que conforman el Tribunal Electoral del Estado de Jalisco, cabe señalar que cuando el Órgano Jurisdiccional se encuentre en proceso electoral,



las capacitaciones quedan suspendidas hasta la culminación de los términos, para el cumplimiento del Proceso Electoral.

Así mismo cuando por necesidades en particular de cada área o por el ingreso de nuevo personal, se solicitará a las instancias correspondientes capacitaciones extraordinarias.

### ÁREAS A CAPACITAR

ÁREA	PERSONAL
Ponencias de los Magistrados	Magistrados, Secretario Relator, Operador Administrativo, Asistente Judicial y Secretaria
Secretaría General, Departamento de Oficialía de Partes, Actuaría y Archivo, Jurídico, Secretaría Técnica y Órgano de Control Interno.	Secretario Técnico, Jefe de Departamento, Jefe de Sección, Jefe de Oficina, Asistente Judicial y Secretaria.
Instituto de Investigaciones y Capacitación Electoral	Director, Secretario Académico, Secretario Administrativo y Asistente Administrativo.
Dirección General de Administración, Recursos Humanos, Materiales y Servicios Generales. Departamento de Contabilidad y Presupuesto, Jefatura de Informática y Jefatura de Comunicación Social.	Directora, Jefe de Departamento, Jefe de Oficina, Contadores, Operador Administrativo, Secretarías y Auxiliares en cómputo.
Unidad de Transparencia y Protección de Datos Personales	Jefe de Sección, Asistente Administrativo y Secretaria.  <b>NOTA:</b> Los integrantes de la Unidad de Transparencia estarán presentes en todas las capacitaciones que se brinden al personal del Tribunal Electoral, así como, asistir de acuerdo a las necesidades a las convocatorias para Especialidades, Diplomados, Talleres, cursos y demás actividades de capacitación en la materia.

### SESIONES DE CAPACITACIÓN

Las sesiones serán de dos horas, esto a efecto de no interferir en las actividades inherentes al proceso jurisdiccional y administrativo, que se lleva a cabo en el Tribunal Electoral del Estado de Jalisco.

### TEMAS DE CAPACITACIÓN



- "Generalidades de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados"
- "Principios y Deberes de Protección de Datos Personales en Posesión de Sujetos Obligados".
- Sistema de Gestión, Medidas de seguridad y acciones preventivas de Protección de Datos Personales en Posesión de Sujetos Obligados".

## CATÁLOGO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

**Expedientes laborales personales de los Servidores Públicos que laboran en el Tribunal Electoral del Estado de Jalisco.**

SISTEMA DE TRATAMIENTO			
Administrador	Armando Salvador Pelayo Alfaro	Bases de datos	N/A
Cargo:	Encargado de Despacho del Departamento de Recursos Humanos y Servicios Generales		
Área	Dirección General de Administración, Recursos Humanos, Materiales y Servicios Generales		
Funciones y obligaciones	<p>I. Ejecutar los sistemas de administración y desarrollo de personal;</p> <p>II. Realizar las actividades administrativas necesarias relacionadas con la elaboración del nombramiento y control de personal que labore para el Tribunal Electoral, conforme a los lineamientos que dicte el Pleno o la Presidencia del Tribunal;</p> <p>III. Llevar a cabo el sistema de remuneraciones al personal de conformidad con los catálogos de puestos, tabuladores de sueldos y presupuestos autorizados;</p>		

IV. Analizar la procedencia de las licencias con goce o no de sueldo, a los servidores públicos; V. Efectuar las reubicaciones y cambios de adscripción del personal, cuando así le sea instruido;

VI. Llevar el control de los períodos de vacaciones escalonados autorizados a los servidores públicos;

VII. Proponer a la Dirección General, de entre los servidores públicos que laboran para el Tribunal Electoral, candidatos para la aplicación de los sistemas de premios, estímulos y recompensas al personal, con base en la normativa aplicable;

VIII. Participar, en su caso, en los comités y comisiones que determine el Pleno;

IX. Operar o auxiliar en su caso, el sistema de pago de nómina en coordinación con la Dirección General;

X. Integrar el expediente de declaraciones, respecto a las retenciones y aportaciones del Impuesto sobre la Renta, del Instituto Mexicano del Seguro Social y Pensiones del Estado u otros semejantes;

XI. Mantener actualizadas las plantillas de personal de todas las áreas del Tribunal Electoral, conforme a las partidas autorizadas en el presupuesto vigente para la elaboración de las nóminas de sueldos y remuneraciones;

XII. Realizar el proceso de elaboración de nómina de sueldos y remuneraciones diversas, así como verificar el control de pagos de las áreas del Tribunal Electoral;

XIII. Actualizar el archivo vigente de nóminas de sueldos y remuneraciones diversas, atendiendo a los movimientos e incidencias del personal en las áreas del Tribunal Electoral para su autorización y elaboración;

XIV. Presentar el diagnóstico de operación de las instalaciones, mobiliario y equipamiento de las dependencias del Tribunal Electoral al Director de su área en forma continua;



XV. Elaborar los programas de requerimientos necesarios y mantenimiento preventivo y correctivo de las instalaciones, mobiliario y equipamiento de las dependencias del Tribunal Electoral para determinar sus costos;

XVI. Conservar y dar mantenimiento a las instalaciones, mobiliario y equipamiento del Tribunal Electoral que se utilice para su actividad;

XVII. Verificar, y en su caso, validar los requerimientos de pago de gastos diversos, conforme a las partidas autorizadas, instrumentando para ello procedimientos de control interno;

XVIII. Coordinar la correcta utilización y mantenimiento de los vehículos del Tribunal Electoral, asignados a diversas áreas para el uso moderado y adecuado a su función oficial;

XIX. Promover entre el personal y el usuario de los servicios del Tribunal Electoral, las acciones preventivas para la mejor conservación de las instalaciones del Tribunal;

XX. Mantener el aseo de las instalaciones del Tribunal Electoral, coordinando al personal de intendencia;

XXI. Apoyar a las áreas jurisdiccionales y administrativas del Tribunal Electoral en servicios de mensajería y transportación de elementos, indispensables para el ejercicio de sus funciones;

XXII. Coadyuvar con la Dirección General y con el apoyo de seguridad y vigilancia, en la corrección de cualquier anomalía detectada en las diversas instalaciones del Tribunal Electoral;

XXIII. Verificar el cuidado de los bienes asignados fuera de los horarios de servicio y en general, todos los muebles, enseres y útiles del Tribunal Electoral;

XXIV. Colaborar con la Dirección General en la implementación de programas de seguridad y prevención de accidentes; y,

XXV. Las demás que le sean asignadas por la Dirección General, en el ámbito de su competencia. En el ejercicio de sus obligaciones deberá observar las disposiciones en materia



	laboral que corresponda ejercer al Tribunal Electoral, siempre en observancia de las leyes, reglamentos y demás normativas aplicables.
<b>Tipo de datos personales pertenecientes al sistema de tratamiento</b>	
<b>Inventario:</b>	<b>Datos de identificación:</b> ELIMINADO: cuatro renglones, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Datos personales resguardados. Indicaría la condición y tipo de datos y se podría encontrar puntos débiles.
	<b>Datos de salud:</b> ELIMINADO: un renglón, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Datos personales resguardados. Indicaría la condición y tipo de datos y se podría encontrar puntos débiles.
	<b>Datos académicos:</b> ELIMINADO: dos renglones, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Datos personales resguardados. Indicaría la condición y tipo de datos y se podría encontrar puntos débiles.
	<b>Datos laborales:</b> ELIMINADO: cinco renglones, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Datos personales resguardados. Indicaría la condición y tipo de datos y se podría encontrar puntos débiles.
	<b>Datos patrimoniales:</b> ELIMINADO: dos renglones, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Datos personales resguardados y bases de datos existentes. Indicaría la condición y tipo de datos y se podría encontrar puntos débiles para vulnerarlos.
<b>Bases de datos</b>	
<b>Controles de seguridad para las bases de datos</b>	<ul style="list-style-type: none"> <li>ELIMINADO: tres renglones, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Controles de Seguridad de los datos personales. Indicaría la condición de los datos y se podrían encontrar puntos débiles.</li> </ul>
<b>Estructura y descripción del Sistema de tratamiento</b>	
<b>Tipo de soporte:</b>	Físico
<b>Características del lugar de resguardo:</b>	<ul style="list-style-type: none"> <li>ELIMINADO: dos renglones, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Características del lugar de resguardo. Indicaría la condición de los datos y se podría encontrar puntos débiles.</li> </ul>
<b>Programas en que se utilizan los D.P.</b>	Excel



## Padrón de Proveedores del Tribunal Electoral del Estado de Jalisco.

SISTEMA DE TRATAMIENTO			
Administrador	Guadalupe Araceli Muñoz Murillo	Bases de datos	N/A
Cargo:	Jefe de Departamento de Recursos Materiales y Patrimoniales		
Área	Dirección General de Administración, Recursos Humanos, Materiales y Servicios Generales		
Funciones y obligaciones	<p>I. Realizar los dictámenes, opiniones, estudios e informes que le sean solicitados por la Presidencia o el Pleno;</p> <p>II. Llevar a cabo los trámites necesarios, para realizar las adquisiciones de los artículos de consumo destinados al Tribunal Electoral, conforme al procedimiento aprobado por el Pleno, el Comité de Adquisiciones, la Comisión de Compras y Contratación de Servicios o el Presidente;</p> <p>III. Efectuar los trámites inherentes para las adquisiciones de artículos de activo fijo, conforme a las disposiciones que para ese efecto le hayan sido ordenadas por el Pleno, el Comité de Adquisiciones, la Comisión de Compras y Contratación de Servicios o el Presidente;</p> <p>IV. Formular el anteproyecto anual de las adquisiciones del Tribunal Electoral, a fin de administrar su distribución de acuerdo a las prioridades establecidas en los programas de actividades y en su caso ajustar los programas de adquisiciones a las partidas autorizadas;</p> <p>V. Elaborar y presentar al Presidente para su análisis y aprobación los proyectos de reglamentos, manuales de organización, procedimientos y servicios de la dirección a su cargo;</p>		

VI. Proporcionar la información y cooperación técnica, solicitada por la Dirección de Administración, departamentos y oficinas de este Tribunal;

VII. Participar como Secretario Técnico en la Comisión de Compras y Contratación de Servicios y formular las observaciones que considere necesarias, así como proporcionar la información que le sea requerida;

VIII. Controlar las requisiciones y en su caso, las órdenes de compra de acuerdo con las autorizaciones respectivas;

IX. Mantener actualizadas en forma mensual las estadísticas de consumo;

X. Realizar quincenalmente los inventarios y controlar las existencias de almacén;

XI. Conservar y resguardar los archivos que contengan la documentación relacionada con las compras de los insumos, bienes y servicios que se hayan destinado al Tribunal Electoral, cuando menos por un período de diez años;

XII. Proporcionar la asesoría que le sea solicitada por los Magistrados o los servidores públicos del Tribunal, así como despachar los asuntos del Órgano Interno de Control en ausencia de su titular;

XIII. Verificar la eficaz aplicación de los acuerdos que ordene el Pleno en el área de su competencia;

XIV. Realizar mensualmente la cédula de depreciaciones de activo y remitirla a la Dirección General, a más tardar el día cinco de cada mes, para su incorporación en estados financieros;

XV. Proponer los sistemas viables para los procedimientos de control interno, los que una vez aprobados, serán implementados;

XVI. Realizar el inventario de los bienes muebles e inmuebles y vigilar su conservación;

XVII. Elaborar el resguardo de los bienes materiales que



	<p>cada servidor público tenga asignado para el cumplimiento de la función que desempeña y llevar el control y archivo de los mismos;</p> <p>XVIII. Vigilar que los servidores públicos brinden el uso adecuado a las instalaciones, mobiliario y equipo que les fue asignado para el cumplimiento de sus funciones y;</p> <p>XIX. Las demás que le confieran este Reglamento o que le sean encomendadas por la Presidencia o el Pleno, le sean asignadas por la Dirección General, en el ámbito de su competencia. En el ejercicio de sus obligaciones deberá observar las disposiciones en materia financiera, contable, presupuestal, fiscal, laboral, de adquisiciones y arrendamientos de bienes y servicios destinados al uso propio del Tribunal Electoral, siempre en observancia de las leyes, reglamentos y demás normativas aplicables.</p>
<b>Tipo de datos personales pertenecientes al sistema de tratamiento</b>	
<b>Inventario:</b>	<p><b>Datos académicos:</b></p> <p><b>Datos de identificación:</b></p> <div data-bbox="954 1087 1369 1312"> <p>ELIMINADO: cuatro renglones, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Datos personales resguardados. Indicaría la condición y tipo de datos y se podría encontrar puntos débiles.</p> </div>
<b>Bases de datos</b>	<div data-bbox="646 1360 1377 1507"> <p>ELIMINADO: un renglón, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Bases de datos existentes. Indicaría la condición y tipo de datos y se podría encontrar puntos débiles para vulnerarlos.</p> </div>
<b>Controles de seguridad para las bases de datos</b>	<ul style="list-style-type: none"> <li>• <div data-bbox="678 1549 1369 1732"> <p>ELIMINADO: tres renglones, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Controles de Seguridad de los datos personales. Indicaría la condición de los datos y se podrían encontrar puntos débiles.</p> </div></li> </ul>
<b>Estructura y descripción del Sistema de tratamiento</b>	
<b>Tipo de soporte:</b>	<b>Físico</b>



<b>Características del lugar de resguardo:</b>	<ul style="list-style-type: none"> <li>• ELIMINADO: tres renglones, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Características del lugar de resguardo. Indicaría la condición de los datos y se podría encontrar puntos débiles.</li> </ul>
<b>Programas en que se utilizan los D.P.</b>	Word, Excel

## EXPEDIENTES ADMINISTRATIVOS DE LOS ALUMNOS Y EXALUMNOS DEL INSTITUTO DE INVESTIGACIÓN Y CAPACITACIÓN DEL TRIBUNAL ELECTORAL DEL ESTADO DE JALISCO.

SISTEMA DE TRATAMIENTO			
<b>Administrador</b>	Luis Rafael Montes de Oca Valadez	<b>Bases de datos</b>	N/A
<b>Cargo:</b>	Director del Instituto de Investigación y Capacitación Electoral		
<b>Área</b>	Instituto de Investigación y Capacitación Electoral		
<b>Funciones y obligaciones</b>	<p>I. Elaborar el proyecto del programa general de actividades y presentarlo para su autorización al Pleno;</p> <p>II. Organizar y coordinar investigaciones orientadas a la comprensión del fenómeno político, cultura cívica, política y electoral;</p> <p>III. Organizar y coordinar investigaciones tendientes a la optimización de la función jurisdiccional y la normativa electoral, con el fin de perfeccionar y fortalecer los instrumentos democráticos en la Entidad;</p> <p>IV. Coordinar la impartición de programas de educación superior, cursos de capacitación, talleres, diplomados, seminarios, foros, congresos; así como otras actividades docentes que estén vinculadas al Derecho Electoral, que considere necesarios y que en su caso, le hayan sido solicitados. Estando facultado para expedir y firmar las actas, grados, títulos, certificados, constancias o diplomas, correspondientes a cada uno de los estudios ofertados.</p> <p>V. Promover el desarrollo de la vocación de servicio, así</p>		



como el ejercicio de los valores éticos y principios jurídicos inherentes a la función judicial, organizando talleres, cursos o conferencias de especialistas en la materia;

VI. Divulgar a través de la edición y publicación de investigaciones que fortalezcan el conocimiento en materia electoral en sus áreas teóricas y contenciosas, así como la educación cívica y la cultura democrática, a través de la realización de jornadas didácticas, con el objeto de contribuir al fomento de la cultura político-jurídica en la entidad;

VII. Fomentar la participación de los servidores públicos de este Tribunal Electoral en actos académicos de investigación y capacitación, ya sea internos o externos que celebren otros organismos o instituciones;

VIII. Elaborar y desarrollar las actividades docentes contempladas en el programa general de actividades, con el objeto de capacitar al personal jurídico del Tribunal Electoral para su permanente actualización; y,

IX. Las demás atribuciones que le impongan el Pleno, este Reglamento y las demás disposiciones legales aplicables.

El Director podrá organizar planes de estudio a cursos propedéuticos para los servidores públicos del Tribunal Electoral, en el año anterior al de la elección, que incluya cuando menos:

a) El conocimiento práctico de los trámites, diligencias y actuaciones que se llevan a cabo en la tramitación y Sustanciación de los medios de impugnación, competencia del Tribunal Electoral;

b) El perfeccionamiento de las habilidades y técnicas en materia de elaboración de actuaciones judiciales e integración de expedientes;

c) La actualización y aplicación de los conocimientos respecto de las legislaciones aplicables, doctrina y jurisprudencia en materia electoral; y,

d) Las técnicas de argumentación en la elaboración de





**TRIBUNAL  
ELECTORAL**  
DEL ESTADO DE JALISCO

	sentencias.
<b>Tipo de datos personales pertenecientes al sistema de tratamiento de los datos personales.</b>	
<b>Inventario:</b>	<div><div><b>Datos académicos:</b></div><div><b>Datos de identificación:</b></div><div>ELIMINADO: cuatro renglones, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Datos personales resguardados. Indicaría la condición y tipo de datos y se podría encontrar puntos débiles.</div></div>
<b>Bases de datos</b>	ELIMINADO: un renglón, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Bases de datos existentes. Indicaría la condición y tipo de datos y se podría encontrar puntos débiles para vulnerarlos.
<b>Controles de seguridad para las bases de datos</b>	<ul style="list-style-type: none"><li>ELIMINADO: dos renglones, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Controles de Seguridad de los datos personales. Indicaría la condición de los datos y se podrían encontrar puntos débiles.</li></ul>
<b>Estructura y descripción del Sistema de tratamiento</b>	
<b>Tipo de soporte:</b>	Físico
<b>Características del lugar de resguardo:</b>	<ul style="list-style-type: none"><li>ELIMINADO: tres renglones, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Características del lugar de resguardo. Indicaría la condición de los datos y se podría encontrar puntos débiles.</li></ul>
<b>Programas en que se utilizan los D.P.</b>	Word, Excel
<b>Resguardo de los soportes físicos y/o electrónicos en que se encuentran los datos personales</b>	
<b>Físicos</b>	ELIMINADO: dos párrafos, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Características del lugar de resguardo. Indicaría la condición de los datos y se podría encontrar puntos débiles.



## Declaraciones Patrimoniales históricas de los Servidores Públicos del Tribunal Electoral del Estado de Jalisco.

SISTEMA DE TRATAMIENTO			
Administrador	Guadalupe Araceli Muñoz Murillo	Bases de datos	N/A
Cargo:	Encargada de despacho.		
Área	Órgano Interno de Control		
Funciones y obligaciones	<p>I. Programar, organizar, dirigir, controlar y evaluar el desempeño de las labores encomendadas a la Jefatura a su cargo;</p> <p>II. Acordar con el Presidente del Tribunal la resolución de los asuntos, cuya tramitación corresponda a la Jefatura a su cargo e informar el avance de los programas de trabajo y de las irregularidades derivadas de las revisiones;</p> <p>III. Realizar los dictámenes, opiniones, estudios e informes que le sean solicitados por la Presidencia o el Pleno;</p> <p>IV. Elaborar y presentar al Presidente para su análisis y aprobación los proyectos de reglamentos, manuales de organización, procedimientos y servicios de la Jefatura a su cargo;</p> <p>V. Proporcionar la asesoría que le sea solicitada por los Magistrados o los servidores públicos del Tribunal;</p> <p>VI. Formar parte de la estructura del comité de adquisiciones en términos que establece la Ley de Compras Gubernamentales, Enajenaciones y contratación de servicios del Estado de Jalisco y sus Municipio;</p> <p>VII. Elaborar y presentar al Presidente para su análisis y aprobación la Matriz de Indicadores para integrarse al presupuesto de egresos anual;</p> <p>VIII. Realizar el seguimiento y evaluación de los resultados</p>		

obtenidos de la Matriz de Indicadores en los plazos establecidos en la normatividad aplicable;

IX. Verificar la aplicación de los acuerdos que ordene el Pleno en el área de su competencia;

X. Elaborar el programa anual de trabajo para las revisiones en la forma y términos que le sean requeridos por el Pleno o el Presidente, siguiendo las normas y lineamientos aplicables en la materia;

XI. Aplicar el programa anual de trabajo y los programas específicos para las revisiones y sus resultados;

XII. Establecer e implementar, conjuntamente con la Dirección General de Administración, las acciones correctivas que se requieren como resultado de las revisiones practicadas;

XIII. Verificar la correcta operación en materia de contratación, pago de los recursos y obras, adquisiciones y afectaciones, enajenación de bienes muebles e inmuebles, abastecimiento y control de suministros y servicios;

XIV. Entregar los formatos declaración de situación patrimonial a los servidores públicos del Tribunal Electoral que por ley les corresponda presentarla;

XV. Brindar asesoría, orientación y apoyo a los servidores públicos en el llenado del formato correspondiente de declaración de situación patrimonial;

XVI. Proponer los sistemas viables para los procedimientos de control interno, los que una vez aprobados, serán implementados y;

XVII. Las demás que le confieran este Reglamento o que le sean encomendadas por la Presidencia o el Pleno, en el ámbito de sus respectivas competencias.

En el ejercicio de sus atribuciones deberá observar las disposiciones en materia financiera, contable, presupuestal, fiscal y de adquisiciones que corresponda ejercer al Tribunal Electoral, siempre en observancia de las leyes, reglamentos y demás normativas aplicables.



Tipo de datos personales pertenecientes al sistema de tratamiento de datos personales.	
Inventario:	<p><b>Datos contenidos en la declaración patrimonial:</b></p> <p>ELIMINADO: un párrafo, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Datos personales resguardados. Indicaría la condición y tipo de datos y se podría encontrar puntos débiles o incentivar a acceder a ellos.</p>
Bases de datos	<p>ELIMINADO: un renglón, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Bases de datos existentes. Indicaría la condición y tipo de datos y se podría encontrar puntos débiles para vulnerarlos.</p>
Controles de seguridad para las bases de datos	<ul style="list-style-type: none"> <li>ELIMINADO: dos renglones, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Controles de Seguridad de los datos personales. Indicaría la condición de los datos y se podrían encontrar puntos débiles.</li> </ul>
Estructura y descripción del Sistema de tratamiento	
Tipo de soporte:	Físico
Características del lugar de resguardo:	ELIMINADO: tres renglones, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Características del lugar de resguardo. Indicaría la condición de los datos y se podría encontrar puntos débiles.
Programas en que se utilizan los D.P.	Word, Excel
Resguardo de los soportes físicos y/o electrónicos en que se encuentran los datos personales	
Físicos	ELIMINADO: dos párrafos, Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Características del lugar de resguardo. Indicaría la condición de los datos y se podría encontrar puntos débiles.

**Unidad de Transparencia y Protección de Datos Personales del  
Tribunal Electoral del Estado de Jalisco.**

# ANEXO 1

## Formato A

### FORMATO A

#### Vulneraciones a los Sistemas de Información y Bases de Datos

CONTENIDO DE LA BITACORA	COMPLETE EL CONTENIDO DE LA BITACORA
FECHA DEL INCIDENTE	Haga clic aquí para escribir una fecha.
NOMBRE	
CARGO	
AREA	
RESPONSABLE DEL AREA	
CAUSA DE LA VULNERACIÓN	
SISTEMA(S) DE INFORMACIÓN O BASE(S) DE DATO(S) VULNERAD(O)	
CANTIDAD DE TITULARES	
SOPORTE DE LA INFORMACIÓN VULNERADA	<input type="checkbox"/> Físico <input type="checkbox"/> Electrónico <input type="checkbox"/> Mixto
SELECCIONE EL TIPO DE VULNERACIÓN	<input type="checkbox"/> Pérdida o destrucción no autorizada <input type="checkbox"/> Robo, extravío o copia no autorizada <input type="checkbox"/> Uso, acceso o tratamiento no autorizado <input type="checkbox"/> Daño, alteración o modificación no autorizada
TIPO DE DATOS PERSONALES COMPROMETIDOS	<input type="checkbox"/> Identificativos <input type="checkbox"/> Laborales <input type="checkbox"/> Tránsito y Movimientos Migratorios <input type="checkbox"/> Académicos <input type="checkbox"/> Procedimientos Administrativos o Judiciales <input type="checkbox"/> Patrimonial <input type="checkbox"/> Salud <input type="checkbox"/> Ideológicos <input type="checkbox"/> De origen <input type="checkbox"/> Características Personales <input type="checkbox"/> Vida Sexual
Nombre y firma de quién reporta	Nombre y firma del administrador del sistema
	Nombre y firma del titular del área



# ANEXO 2

## Formato B

### FORMATO B

#### Vulneraciones a los Sistemas de Información y Bases de Datos

CONTENIDO DE LA BITACORA	COMPLETE EL CONTENIDO DE LA BITACORA
FECHA DEL INCIDENTE	Haga clic aquí para escribir una fecha.
NOMBRE DEL RESPONSABLE DE LA INVESTIGACIÓN	
CARGO	
AREA	
NÚMERO DE INVESTIGACIÓN	
LA INFORMACIÓN VULNERADA ESTA REGISTRADA EN EL DOCUMENTO DE SEGURIDAD	<input type="checkbox"/> Sí <input type="checkbox"/> No
EN CASO DE QUE LA INFORMACIÓN NO ESTUVIERA VULNERADA, SOLICITE AL RESPONSABLE DEL ÁREA UN INFORME AL RESPECTO CON EL OBJETO DE RESPONDER EL CONTENIDO DEL APARTADO A.	
<b>APARTADO A</b>	
FECHA EN QUE SE CREO EL SISTEMA DE INFORMACIÓN O BASE DE DATOS VULNERADA	Haga clic aquí para escribir una fecha.
FUNDAMENTO LEGAL PARA OBTENCIÓN DE LOS DATOS PERSONALES.	
RESGUARDO DE LOS SOPORTES	
USUARIOS	
MEDIDAS DE SEGURIDAD FÍSICAS TÉCNICAS Y ADMINISTRATIVAS APLICADAS	
LAS CAUSAS ENUNCIADAS EN EL FORMATO A	
LO QUE EL TITULAR DEL ÁREA CONSIDERE PERTINENTE	
<b>APARTADO B</b>	
ADMINISTRADOR DEL SISTEMA(S) DE INFORMACIÓN O BASE(S) DE DATOS VULNERADO (S)	
USUARIOS DEL SISTEMA(S) DE INFORMACIÓN O BASE(S) DE DATOS VULNERADO (S)	
LOS HECHOS DE MODO TIEMPO Y LUGAR ENUNCIADOS EN EL FORMATO A	
RESGUARDANTE SOPORTE FÍSICO O ELECTRÓNICO VULNERADO	







## **Políticas Internas de Gestión y Tratamiento de Datos Personales del Tribunal Electoral del Estado de Jalisco**

### **Contenido**

1. Objetivo.
2. Fundamento legal.
3. Ámbito de aplicación.
4. Disposiciones generales.
5. Controles para garantizar que se valida la confidencialidad, integridad y disponibilidad de los datos personales.
  - 5.1 Controles de Confidencialidad.
  - 5.2. Controles de Integridad.
  - 5.3. Controles de Disponibilidad.
6. Acciones para restaurar la disponibilidad y el acceso a los datos personales de manera oportuna en caso de un incidente físico o técnico.
7. Medidas correctivas en caso de identificar una vulneración o incidente en los tratamientos de datos personales.
8. Proceso para evaluar periódicamente las políticas, procedimientos y planes de seguridad establecidos, a efecto de mantener su eficacia.
9. Controles para garantizar que únicamente el personal autorizado podrá tener acceso a los datos personales para las finalidades concretas, lícitas, explícitas y legítimas que originaron su tratamiento.
10. Medidas preventivas para proteger los datos personales contra su destrucción accidental o ilícita, su pérdida o alteración y el almacenamiento, tratamiento, acceso o transferencias no autorizadas o acciones que contravengan las disposiciones normativas en materia de protección de datos personales.

## **1. Objetivo.**

Establecer los principios generales o criterios de acción que servirán de guía en el proceso de toma de decisiones y en la actuación de los servidores públicos al ejecutar los objetivos institucionales en materia de protección de datos personales al interior del Tribunal Electoral del Estado de Jalisco.

## **2. Fundamento legal.**

De conformidad con el artículo 32, fracción I de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, el Tribunal Electoral del Estado de Jalisco, tiene el deber establecer y mantener las medidas de seguridad para la protección de los datos personales, mediante una serie de acciones interrelacionadas, entre dichas acciones se encuentra el crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión.

## **3. Ámbito de aplicación**

Las políticas contenidas en el presente documento son de aplicación general para todos aquellos servidores públicos del Tribunal Electoral del Estado de Jalisco, que en el ejercicio de sus funciones obtengan, usen, registren, organicen, conserven, elaboren, utilicen, comuniquen, difundan, almacenen, posean, manejen, aprovechen, divulguen, transfieran o dispongan de datos personales

## **4. Disposiciones generales**

a) El uso, recolección y tratamiento de datos personales por parte del Tribunal Electoral del Estado de Jalisco, se fundamenta en las siguientes normativas:

- Constitución Política del Estado de Jalisco: artículos 4º y 9º fracción II, V y del 68 al 71.
- Código Electoral del Estado de Jalisco artículo 507, fracciones I, II, III, IV, VI, VIII, IX, X, artículo 515, fracciones I, II, III, IV, V, artículo 520 párrafo 1, artículo 521 párrafo 1, artículo 530 párrafo 1, fracciones I, II, III, IV, VI, VII, 548 párrafo 1, artículo 549 párrafo 1, 551 párrafo 1, fracciones III, IV y párrafo 2, artículo 617 párrafo 1 fracción I, V, artículo 620 fracción 1 y artículo 661 párrafo 1, fracción I, V, VI.
- Ley General de Responsabilidades Administrativas, artículos 32 y 33.



- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, artículos 3, fracciones II, VIII, IX, X y XXXIII, 17, 18, 19, 21, 22, 23, 25 al 28 y 84.
- Ley de Responsabilidades Políticas y Administrativas del Estado de Jalisco, artículos 3, fracción VII; 51, 52 y 54.
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados Del Estado de Jalisco y sus Municipios: artículos 3, párrafo 1, fracciones III, VIII, IX, X, XI, XXXII, XXXV, XXXVI y XXXVII, 10, 11, 13, 14, 19, 20 al 26, 28, 74, 75 y 87.
- Ley para los Servidores Públicos del Estado de Jalisco y sus Municipios artículo 17 fracción I, artículo 54 bis-4, 54 bis-5, 56 fracciones IV, XII, XIV, XVI y XVIII, y artículo 64.
- Ley General de Transparencia y Acceso a la Información Pública: artículo 116.
- La Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios: artículos 3º, párrafo 2, fracción II inciso a), 8º, 11-Bis, 20, 21, 22, 23 y 66.
- Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios, artículos 5, 7, 8, párrafo 2, 14, 19, 20 y 82
- Reglamento de la Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios, artículos 6 y 16
- Reglamento Interno del Tribunal Electoral del Estado de Jalisco: artículos 2, fracción V, VI y VII, 58, fracción III, 134, 135 y 136.
- Reglamento Interno de Transparencia, y Acceso a la Información Pública del Tribunal Electoral del Estado de Jalisco: artículos 1, 4, 22, 23 y 24.
- Reglamento de Posgrado en Derecho Electoral del Instituto de Investigaciones y Capacitación Electoral artículos 11, 13, 15, 19 y 20.
- Lineamientos Generales para la Clasificación, Desclasificación y Custodia de la Información Reservada y Confidencial, que deberán Observar los Sujetos Obligados Previstos en el artículo 3 de la Ley de Transparencia e Información Pública del Estado de Jalisco, numeral cuadragésimo octavo y cuadragésimo noveno.

- Lineamientos Generales para la Protección de la Información Confidencial y Reservada emitidos por el Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco: numeral décimo quinto, décimo sexto, décimo séptimo y quincuagésimo octavo, fracciones I, II, III y IV.
- b) El tratamiento de datos personales deberá sujetarse a las facultades o atribuciones que la normatividad aplicable confiere al y estar justificado por finalidades concretas, lícitas, explícitas y legítimas.
- c) Únicamente se podrán tratar datos personales para finalidades distintas a las establecidas en el aviso de privacidad, siempre que se cuente con atribuciones y medie el consentimiento del titular de dichos datos.
- d) Previo a recabar datos personales, se deberá mostrar el Aviso de Privacidad Integral del Tribunal Electoral del Estado de Jalisco, mismo que debe encontrarse en todas las áreas administrativas que recaben datos personales.
- e) Cuando se recaben datos personales sensibles, de conformidad a lo establecido en el artículo 3, fracción X, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, deberá obtenerse el consentimiento expreso, con nombre y firma autógrafa de los titulares.
- f) Cuando se recaben datos personales de menores deberá obtenerse el consentimiento expreso, con nombre y firma autógrafa de quienes ejerzan la patria potestad o tutela sobre éstos.
- g) No deberán obtenerse y tratar datos personales, a través de medios engañosos o fraudulentos.
- h) Se deberán adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales que se reciban en ejercicio de las facultades otorgadas.
- i) Se deberá limitarse al mínimo posible, la obtención de datos de manera indirecta del titular.
- j) Cuando se recaben datos de manera indirecta del titular, deberá ponerse a disposición de los titulares el aviso de privacidad previo al aprovechamiento de los mismos.



k) El derecho a la protección de los datos personales solamente se limitará por lo establecido en el artículo 5 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

l) Únicamente se deberán tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para el ejercicio de las facultades o atribuciones del Tribunal Electoral del Estado de Jalisco.

m) Las y los servidores públicos del Tribunal Electoral del Estado de Jalisco que administren, actualicen o tengan acceso a bases de datos que contengan datos personales, se comprometen a conservar, manejar y mantener de manera estrictamente confidencial dicha información y no revelarla a terceros.

## **5. Controles para garantizar que se valida la confidencialidad, integridad y disponibilidad de los datos personales.**

El artículo 30 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios establece que los responsables deben garantizar la confidencialidad, integridad y disponibilidad de los datos personales en su posesión.

### **5.1 Controles de Confidencialidad.**

- El personal del Tribunal Electoral del Estado de Jalisco deberá guardar confidencialidad permanente de los datos personales a los que tenga acceso.
- Se podrán desclasificar datos personales solo en los casos que la Leyes en la materia señalen.
- El Tribunal Electoral del Estado de Jalisco impartirá capacitaciones periódicas para todo su personal, en materia de protección de datos personales.
- El personal está obligado a cumplir con las medidas de seguridad físicas, técnicas y administrativas señaladas en el Documento de Seguridad.
- Se realizará una revisión periódica de las medidas de seguridad; físicas, técnicas y administrativas del Tribunal.

### **5.2. Controles de Integridad**

Los datos personales deberán conservarse en el estado en que son recabados, asimismo los documentos que resulten del aprovechamiento de los datos personales deberán conservar su integridad.

El personal conservará los datos personales que se encuentren en formato físico conforme a lo señalado por las medidas de seguridad físicas contenidas en el Documento de Seguridad.

El personal conservará los datos personales que se encuentren en formato electrónico conforme a lo señalado por las medidas de seguridad técnicas contenidas en el Documento de Seguridad.

### 5.3. Controles de Disponibilidad.

Se realizará una operación de respaldo incremental solo copia los datos que han variado desde la última operación de respaldo de cualquier tipo. Se utiliza la hora y fecha de modificación estampada en los archivos, comparándola con la hora y fecha del último respaldo.

Cada área será la responsable de almacenar sus respaldos durante el tiempo que señale el catálogo de disposición documental del Tribunal Electoral del Estado de Jalisco, atendiendo, a las recomendaciones del Área Coordinadora de Archivos del Sistema Institucional de Archivos del Tribunal Electoral del Estado de Jalisco, así como de la Unidad de Transparencia y Protección de Datos Personales.

## **6. Acciones para restaurar la disponibilidad y el acceso a los datos personales de manera oportuna en caso de un incidente físico o técnico.**

Los respaldos incrementales contienen fecha y hora, tanto inicial como final. La recuperación se realizará cruzando la fecha del incidente y el último respaldo.

### 7. Medidas correctivas en caso de identificar una vulneración o incidente en los tratamientos de datos personales.

En caso de detectarse una posible vulneración de dato personal deberá realizarse lo siguiente:

a) Restauración Inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos.



- b) En caso de que la vulneración fuera resultado de la comisión de un delito realizar las denuncias correspondientes.
- c) Llenado de Formato A, señalado en el Documento de Seguridad del Tribunal Electoral del Estado de Jalisco, por parte de la persona que detectó la vulneración.
- d) Llenado de Formato B, señalado en el Documento de Seguridad del Tribunal Electoral del Estado de Jalisco, por parte de la Unidad de Transparencia y Protección de Datos Personales del Tribunal Electoral del Estado de Jalisco.
- e) Determinación de la magnitud de la afectación y elaboración de recomendaciones para los titulares.
- f) Elaboración de Informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Unidad de Transparencia y Protección de Datos Personales del Tribunal Electoral del Estado de Jalisco.
- g) Notificación a titulares en un lapso de 72 horas que de forma significativa vean afectados sus derechos patrimoniales o morales.
- h) Llenado de la bitácora de vulneraciones conforme al artículo 39 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y Municipios.

**8. Proceso para evaluar periódicamente las políticas, procedimientos y planes de seguridad establecidos, a efecto de mantener su eficacia;**

La Unidad de Transparencia y Protección de Datos Personales del Tribunal Electoral del Estado de Jalisco Protección de Datos Personales elaborará un plan anual de evaluación las políticas, procedimientos y planes de seguridad que será presentado, y en su caso, aprobado por Comité de Transparencia del Tribunal Electoral del Estado de Jalisco.

**9. Controles para garantizar que únicamente el personal autorizado podrá tener acceso a los datos personales para las finalidades concretas, lícitas, explícitas y legítimas que originaron su tratamiento.**

Los empleados del Tribunal Electoral del Estado de Jalisco deben portar su identificación institucional que cuenta con la siguiente información:

Al frente:

- Nombre.
- Fotografía.
- Clave de empleado.
- Domicilio del Tribunal.
- Cargo.

Al reverso:

- Vigencia.
- Firma del titular de la institución.
- Firma del Secretario General de Acuerdos.

**10. Medidas preventivas para proteger los datos personales contra su destrucción accidental o ilícita, su pérdida o alteración y el almacenamiento, tratamiento, acceso o transferencias no autorizadas o acciones que contravengan las disposiciones normativas en materia de protección de datos personales.**

Se llevarán a cabo capacitaciones periódicas con el objeto de prevenir acciones que contravengan las disposiciones normativas en materia de protección de datos personales de acuerdo al:

“Programa General de Capacitación del Tribunal Electoral del Estado de Jalisco.





**CRITERIOS GENERALES DE PROTECCIÓN DE INFORMACIÓN  
CONFIDENCIAL Y RESERVADA  
DEL TRIBUNAL ELECTORAL DEL ESTADO DE JALISCO**

**TRIBUNAL  
ELECTORAL**  
DEL ESTADO DE JALISCO

**Capítulo I  
Disposiciones Generales**

**PRIMERO.** El Tribunal Electoral del Estado de Jalisco, con la finalidad de proporcionar certeza a los alcances de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, emite sus criterios protección de información confidencial y reservada, que tienen por objeto establecer los procedimientos que deberán de observar los servidores públicos de este Tribunal para el debido manejo, mantenimiento, seguridad y protección de la información confidencial y reservada.

Los presentes criterios se emiten de acuerdo a la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, así como a los Lineamientos Generales para la Protección de la Información Confidencial y Reservada, emitidos por el Instituto de Transparencia e Información Pública del Estado de Jalisco.

**SEGUNDO.** El Tribunal Electoral, tiene la atribución de expedir a través de su Comité de Clasificación de Información sus criterios generales de protección de información confidencial y reservada, ello acorde a lo dispuesto por los artículos 25 fracción IX inciso c) de la Ley de Transparencia y Acceso a la Información Pública del Estado.

**TERCERO.** Se entiende como "protección", todo acto encaminado a asegurar el buen funcionamiento del manejo y seguridad de la información, que garantiza la no revelación de la información confidencial y reservada en posesión de este Tribunal.

Por información Reservada se entiende la señalada en el artículo 17 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, e Información Confidencial la referida en el artículo 21 del mismo ordenamiento.

**CUARTO.** Los servidores públicos del Tribunal que con motivo de sus labores tengan a su alcance información confidencial y reservada, guardarán el secreto profesional de la misma, aun después de concluida su gestión y/o contratación. Lo mismo sucederá con las personas que sean contratadas bajo cualquier otro régimen.

Así mismo, los servidores públicos del Tribunal que con motivo de sus labores tengan a su alcance información confidencial y reservada, deberán observar las medidas de seguridad establecidas en el capítulo III, de los Lineamientos generales para la Protección de la Información Confidencial y Reservada, expedidos por el Instituto de Transparencia e Información Pública de Jalisco.

**QUINTO.** La aplicación de estos criterios queda a cargo de las áreas de este Tribunal que resguardan la información reservada y/o confidencial, que en lo específico son:

1. Instituto Prisciliano Sánchez;
2. Dirección General de Administración, Recursos Humanos, Materiales y Servicios Generales y sus departamentos;
3. Dirección de Contraloría, Auditoría Interna y Control Patrimonial y sus oficinas; y
4. Archivo del Tribunal.

**SEXTO.** Salvo los casos previstos por el artículo 22 de la Ley de Transparencia y Acceso a la Información, este Tribunal no dará acceso, transmitirá, comercializará, distribuirá o difundirá la información reservada o confidencial a terceros, a menos que se trate de solicitud hecha por autoridad en el ejercicio de sus funciones o medie consentimiento expreso y por escrito del titular de dicha información, de conformidad con el artículo 23 punto 1, fracción IV de la Ley.

**SÉPTIMO.** Los servidores públicos al momento de elaborar sus actas de entrega y recepción al término de sus funciones, deberán incluir un apartado especial en el que se especifiquen los documentos y/o soporte digital o magnético que contiene la información de carácter confidencial.

## Capítulo II

### Protección de la Información Reservada

**OCTAVO.** Para dictaminar si la información tiene el carácter de reservada el Comité de Clasificación, deberán determinar que la misma se encuentra dentro de los supuestos que prevé el artículo 17 de la Ley, además de precisar que la publicidad de la misma causaría un daño presente, probable y específico.

**NOVENO.** La información reservada únicamente deberá ser manejada por el personal directamente involucrado en las labores propias de la generación y manejo de la información.



**DÉCIMO.** La información que tenga el carácter de reservada deberá ser resguardada en un lugar seguro, de manera que no se conserve en archivos de fácil acceso al público.

**DÉCIMO PRIMERO.** La información reservada consistente en el contenido íntegro de cualquier expediente jurisdiccional o procedimiento administrativo, seguidos tanto ante el pleno del tribunal o sus comisiones, que aún no hayan causado estado, su resguardo estará a cargo de la Ponencia o Comisión Sustanciadora o Instructora que conozcan del asunto.

**DÉCIMO SEGUNDO.** Para el supuesto en que los documentos contengan parcialmente información reservada, se deberán expedir una versión pública, en la que se supriman los datos reservados, señalando los fundamentos y motivaciones de esta restricción informativa.

## Capítulo II Protección de la Información Confidencial

**DÉCIMO TERCERO.** Es información confidencial para este Tribunal, la descrita en los artículos 4 punto 1 fracción IV y V, y 21 de la Ley de Transparencia.

A efecto de determinar si la información que posea cualquier sujeto obligado se trata de información confidencial, deberán considerarse las siguientes hipótesis:

a) Que la misma sea concerniente a una persona física, identificada o identificable, debiendo entenderse como identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, y que en razón de su contenido permite acceder al conocimiento de diversos aspectos de la persona, incluso obtener una imagen diversificada y compleja de la misma, apta para establecer perfiles de categorización a través de múltiples operaciones de tratamiento a que puedan ser sometidos, que puedan vincularse entre sí, afectando los datos más frágiles y vulnerables en la esfera del ser humano, a través de la exhibición pública y de la incursión sin consentimiento previo a la vida íntima y familiar.

b) Que los datos de una persona se encuentra contenida en los archivos de este Tribunal y que la misma constituye una asociación entre la información y la persona.

**DÉCIMO CUARTO.** Cuando se solicite información relativa a los datos personales, en todo caso podrá ser proporcionada, si se lleva a cabo el procedimiento de disociación.



**TRIBUNAL  
ELECTORAL**  
DEL ESTADO DE JALISCO

La disociación consiste en el procedimiento por el cual, los datos personales no pueden asociarse a su titular, ni permitir, por su estructura, contenido o grado de difusión, la identificación individual del mismo.

**DÉCIMO QUINTO.** Cuando se reciba información que tenga el carácter de confidencial, se deberá hacer del conocimiento de la persona física o jurídica que entregue dicha información, la existencia del aviso de confidencialidad de este Tribunal.

**DÉCIMO SEXTO.** Los datos personales son irrenunciables, intransferibles e indelegables, por lo que no podrán transmitirse salvo disposición legal o cuando medie el consentimiento del titular y dicha obligación subsistirá aún después de finalizada la relación entre el Tribunal con el titular de los datos personales, así como después de finalizada la relación laboral entre el ente público y el responsable del sistema de información confidencial o los usuarios.

En caso de que fallecimiento del titular de los datos personales, se sujetara a lo previsto por los artículos 17 y 18 del Reglamento.

**DÉCIMO SÉPTIMO.** En el tratamiento particularmente de los datos personales, los sujetos obligados deberán observar los principios de licitud, confidencialidad consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, así como las medidas necesarias para el manejo, mantenimiento, seguridad y protección de dicha información.

**Por principio de licitud** se entenderá toda aquella recolección de datos personales que se realice a través de los medios legales o reglamentarios de cada sujeto obligado previsto para tales efectos.

**El principio de confidencialidad**, consiste en garantizar que exclusivamente la persona interesada puede acceder a los datos personales o, en su caso, el responsable o el usuario del sistema de información confidencial para su tratamiento, así como el deber de secrecía del responsable del sistema de información confidencial, así como de los terceros responsables.

**El principio de consentimiento**, se refiere a la manifestación de voluntad libre, inequívoca, específica e informada, mediante la cual el interesado consiente el tratamiento de sus datos personales. Toda transmisión de datos personales deberá contar con el consentimiento del Titular de los datos, mismo que deberá otorgarse en forma libre, expresa e informada, salvo lo dispuesto en el artículo 22 de la Ley de Transparencia. Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, y/o firma electrónica.

**El principio de información**, consiste en hacer del conocimiento del Titular de los datos, al momento de recabarlos y de forma escrita, el fundamento y motivo de ello, así como finalidades y usos para los cuales se tratarán dichos datos. Igualmente se deberá informar verbalmente a sus titulares la existencia del aviso de confidencialidad.



**Por principio de calidad de los datos personales**, se entiende que el tratamiento de dichos datos deberá ser exacto, adecuado, pertinente y no excesivo, respecto de las atribuciones legales de este Tribunal. Se considera que el tratamiento de datos personales es:

- a) Exacto: Cuando los datos personales se mantienen actualizados de manera tal, que no altere la veracidad de la información que pueda traer como consecuencia que el titular de los datos se vea afectado por dicha situación;
- b) Adecuado: Cuando se observan las medidas de seguridad aplicables;
- e) Pertinente: Cuando es realizado por el personal autorizado para el cumplimiento de las atribuciones de este Tribunal, y
- d) No excesivo: Cuando la información solicitada al titular de los datos es estrictamente la necesaria para cumplir con los fines para los cuales se hubiera recabado.

Para efectos de cumplir con el lineamiento que precede, este Tribunal podrá implementar en la recolección de dicha información, formatos que contengan como requisitos mínimos los señalados anteriormente.

**El Principio de Finalidad**, consiste en que los datos personales recabados deberán ser tratados exclusivamente para la finalidad que fueron obtenidos.

**Principio de Lealtad**, Los servidores públicos que por el desempeño de sus labores deben recolectar datos personales, deberán guiarse por el principio de lealtad, que consiste en la prohibición de recolectar datos en forma contraria a la Ley o por medios fraudulentos, desleales o ilícitos.

**DÉCIMO OCTAVO.** La información confidencial contenida en los expedientes personales de los servidores públicos del Tribunal, proveedores y demás personas relacionadas con el Tribunal quedará bajo custodia de la Dirección de Administración, Recursos Humanos, Materiales y Servicios Generales.

**DÉCIMO NOVENO.** La información confidencial contenida en las declaraciones patrimoniales históricas de los servidores públicos del Tribunal, quedará bajo responsabilidad y custodia de la Dirección de Contraloría, Auditoría Interna y Control Patrimonial y sus oficinas.

Así mismo, la publicitación de dichas declaraciones patrimoniales se hará siempre y cuando se cuente con la autorización previa y específica del servidor público de que se trate, ello acorde a lo dispuesto por el artículo 100 párrafo 3 de la Ley de Responsabilidades de los Servidores Públicos del Estado de Jalisco.



**TRIBUNAL**  
**ELECTORAL**  
DEL ESTADO DE JALISCO

**VIGÉSIMO.** La información confidencial contenida en los expedientes de los alumnos de los posgrados que se imparten en este Tribunal quedará bajo custodia del Instituto Prisciliano Sánchez.

**VIGÉSIMO PRIMERO.** Para la protección de la información confidencial, este Tribunal a través del encargado y/o responsable, tomará, dependiendo del material o soporte en el que se encuentre la información, las siguientes medidas administrativas, físicas y técnicas de seguridad:

I. Dar a conocer los Lineamientos, así como la normatividad relativa al manejo, mantenimiento, seguridad y protección de la información confidencial, que se encuentre en posesión de este Tribunal;

II. Asignar un espacio físico seguro y adecuado para la operación de los sistemas de información confidencial, documentos u otro material en el que se encuentre la misma;

III. Llevar a cabo verificaciones periódicas de la correcta aplicación de las medidas de seguridad que se hayan decidido implementar;

IV. Controlar el acceso a las instalaciones o áreas, donde se encuentra el equipo o el material que soporta información confidencial, llevando un registro de las personas que acceden a ella;

V. Implementación de algoritmos, claves, contraseñas, códigos o candados para el acceso directo a la información confidencial;

VI. Realizar respaldos que permitan garantizar la información confidencial cuando se encuentre en medios magnéticos o digitales;

VII. Realizar las pruebas de las medidas de seguridad que se consideren aplicables, utilizando en paralelo copia de los datos reales, misma que deberá destruirse al final de la prueba;

VIII. Implementar otras medidas de seguridad para el uso de los dispositivos electrónicos y físicos que contengan información confidencial, para evitar el retiro no autorizado de los mismos; y

IX. Llevar un registro de incidencias de las fallas en las medidas de seguridad implementadas.

**VIGÉSIMO SEGUNDO.** No será considerada como una violación de la confidencialidad la publicación del nombre de las partes en los libros de gobierno y estrados de este Tribunal, dado que se trata de un registro público, considerado información pública ordinaria.

**VIGÉSIMO TERCERO.** No será considerada como una violación de la confidencialidad el que las partes, dentro de los procedimientos jurisdiccionales y administrativos conozcan los datos personales de la contraria, tomando en cuenta la naturaleza propia de la relación procesal.



**COMITÉ DE CLASIFICACIÓN DE LA INFORMACIÓN DEL TRIBUNAL  
ELECTORAL DEL ESTADO DE JALISCO**



**Mtro. ÁLVARO ZUNO VÁZQUEZ**

Secretario General del Acuerdos del Tribunal Electoral del Estado de Jalisco; y  
Presidente del Comité de Clasificación de Información Pública.



**Mtra. GUADALUPE LUCÍA  
SÁNCHEZ VITAL**

Titular de la Unidad de Transparencia  
del Tribunal Electoral del Estado de  
Jalisco; y Secretario del Comité de  
Clasificación de Información Pública.



**Lic. PABLO JIMÉNEZ SALAZAR**

Director de Auditoría Interna y Control  
Patrimonial del Tribunal Electoral del  
Estado de Jalisco.



## **CONSTANCIA DE PROTECCIÓN DE INFORMACIÓN CONFIDENCIAL**

Se remite la solicitud de información; misma que contiene información confidencial de acuerdo a lo establecido con el artículo 3, fracción IX de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

En este tenor y en concordancia con el artículo 75, de la Ley antes citada, se transfiere información confidencial a efecto de dar respuesta a la petición del solicitante. Dando cumplimiento a lo establecido en nuestro aviso de privacidad que dispone que los terceros receptores de los datos personales pueden ser; los sujetos obligados a los que se dirijan las solicitudes de información pública que sean de su competencia con la finalidad de darle seguimiento y las diferentes áreas de este sujeto obligado, en caso de que se dé vista por el posible incumplimiento a la Ley que rige la materia.

Por lo que es deber de los receptores salvaguardar en todo momento el derecho a la protección de los datos personales de cada individuo, así como, garantizar su confidencialidad, adquiriendo el carácter de responsable y únicamente los utilizará para los fines que fueron transferidos, atendiendo a lo convenido en el aviso de privacidad<sup>1</sup> que puede consultar en el vínculo electrónico siguiente:

[https://www.recursostriejel.gob.mx/transparencia/aviso\\_privacidad\\_integral.pdf](https://www.recursostriejel.gob.mx/transparencia/aviso_privacidad_integral.pdf)

**CÉSAR OCTAVIO MAGALLANES ESCALERA**  
**JEFE DE DEPARTAMENTO DE LA UNIDAD DE TRANSPARENCIA Y PROTECCIÓN DE DATOS**  
**PERSONALES DEL TRIBUNAL ELECTORAL DEL ESTADO DE JALISCO.**

---

<sup>1</sup> De conformidad a lo dispuesto por los artículos 72 y 74 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Jalisco.