ETZATLÁN
GOBIERNO MUNICIPAL
2024 - 2027

DOCUMENTO DE SEGURIDAD,

PARA LA PROTECCIÓN DE DATOS PERSONALES

Ayuntamiento de Etzatlán, Jalisco.

Administración 2024 - 2027

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.
- **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.
- **Instituto:** Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco.
- **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.
- **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.
- **N/A:** No aplica.
- **Responsable:** Los sujetos obligados señalados en el artículo 1, párrafo 5 de la presente Ley, que determinarán los medios, fines 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:** 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.

SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Después del inventario inicial de datos personales, de las capacitaciones, el cuestionario y diversas gestiones con los enlaces de Transparencia de todas las dependencias del Gobierno Municipal de Etzatlán, Jalisco, se diseñaron 6 sistemas de tratamiento, señalados a continuación:

Trámites y servicios municipales	
Datos de identificación	
Sujeto Obligado	Ayuntamiento de Etzatlán, Jalisco.
Unidades Administrativa Responsables	Todas las áreas que ejecuten trámites. El detalle podrá ser consultado en el Registro de trámites y servicios.
Contenido del sistema	
Finalidad de sistemas y los usos previstos	Obtención de datos personales derivados del comienzo e integración de cualquier expediente dentro del municipio.
Las personas o grupos de personas sobre las cuales se obtienen los datos	Ciudadanos que acuden a realizar trámites.
Procedimien to de recolección	Formatos físicos y electrónicos.
Tipo de soporte en donde se contienen los datos personales	Formatos físicos y electrónicos.
Características del lugar de resguardo	En las oficinas de las áreas generadoras de la información.
Estructura básica del sistema y la descripción de los tipos de datos incluidos	
Datos generales del sistema	
Áreas:	• Órgano Interno de Control:

	• Dirección de Obras Públicas; • Subdirección de Desarrollo Urbano; • Secretaría General; • Sindicatura; • Dirección de Catastro e impuesto predial; • Unidad de Planeación y Gestión Estratégica Municipal; • Dirección de Hacienda Pública Municipal; • Dirección de Adquisiciones; • Dirección de Servicios Públicos Municipales; • Dirección de Rastro Municipal; • Dirección de Desarrollo Económico; • Unidad de Transparencia;
Responsables:	Los y las titulares y/o encargados de área
Contacto:	Pueden consultarse en la siguiente dirección: https://etzatlan.gob.mx/gobierno/directorio-de-extensiones/
Administradores	
Datos personales incluidos en el sistema / inventario	
Tipo de datos personales	Nombre, edad, sexo, fecha de nacimiento, lugar de nacimiento, domicilio particular, correo electrónico personal, teléfonos particulares, credencial electoral, documentos oficiales que acrediten su personalidad, estado civil, firma particular, fotografía, CURP, datos del RFC, cualesquier otro no especificado que sea necesario para el trámite y seguimiento de algún requerimiento de la ciudadanía, o autoridad.
Tipo de tratamiento	Tratamiento no automatizado El que requiera el trámite, siempre y cuando sea lícito, conforme a las nuevas medidas de seguridad.

Cesión de las que puede ser objeto la información confidencial	
Unidades internas, sujetos obligados, autoridades o terceros a los que en su caso se ceden los datos.	El detalle podrá ser consultado en el Registro de trámites y servicios.
Finalidad	Seguimiento y conclusión del trámite iniciado por el ciudadano.
Nivel de protección exigible	
Básico	
Medio	
Alto	X
Normatividad:	
Art. 3, fracción IX de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.	

Programas sociales municipales	
Datos de identificación	
Sujeto Obligado	Ayuntamiento de Etzatlán, Jalisco.
Unidades Administrativas Responsables:	● Dirección de Desarrollo Social; ● Dirección de Desarrollo Rural; ● Dirección de Educación; ● Dirección de Inclusión.
Contenido del sistema	
Finalidad de sistemas y los usos previstos	Organización, preparación y seguimiento de los programas sociales municipales, estatales y federales..
Las personas o grupos de personas sobre las cuales se obtienen los datos	Personas físicas que cumplan con los requisitos para ser beneficiarios de los programas.
Procedimiento de recolección	La recolección se realiza de forma presencial en dicha Dirección.
Tipo de soporte en donde se contienen los datos personales	Formatos físicos y electrónicos.
Características del lugar de resguardo	Archivos electrónicos.

Estructura básica del sistema y la descripción de los tipos de datos incluidos	
Datos generales del sistema	
Responsable	Titular de área en turno
Domicilio	Escobedo No. 320. Colonia Centro. C.P. 46500 Etzatlán , Jalisco
Contacto:	Pueden consultarse en la siguiente dirección: https://etzatlan.gob.mx/gobierno/directorio-de-extensiones/
Administradores	Titulares de área, y Auxiliares
Datos personales incluidos en el sistema / inventario	
Tipo de datos personales	Nombre, edad, fecha de nacimiento, estado civil, nacionalidad, CURP, información familiar, información de sus hijos (nombre, edad, estado de salud y/o discapacidad), información laboral, domicilio particular, número de teléfono particular, estado civil, firma, datos socioeconómicos, estado de salud (enfermedades y/o discapacidades). , cualesquier otro no especificado que sea necesario para el trámite y seguimiento de algún requerimiento de la ciudadanía, o autoridad.
Tipo de tratamiento	Tratamiento no automatizado y automatizado.
Cesión de las que puede ser objeto la información confidencial	
Unidades internas, sujetos obligados, autoridades o terceros a los que en su caso se ceden los datos.	1.- Los Programas Sociales Municipales transfieren información de los beneficiarios a instituciones bancarias para efecto de tramitar una cuenta y/o tarjeta de débito. 2.- En caso de programas sociales estatales, se transfiere el listado de beneficiarios a los entes públicos estatales que dirigen dichos programas sociales.

Finalidad ● Realizar las dispersiones de los apoyos económicos a los beneficiarios. ● Dar cabal y oportuno seguimiento a los programas sociales estatales aplicables en el ámbito municipal.	
Nivel de protección exigible	
Básico	
Medio	
Alto	X
Normatividad:	Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

Contratación de personal	
Unidad Administrativa Responsable	Oficialía Mayor Administrativa
Contenido del sistema	
Finalidad de sistemas y los usos previstos	Dar inicio, seguimiento y conclusión a procedimientos internos que ayudan al correcto desempeño de la Administración Pública Municipal, la contratación de personal, y la celebración de contratos de prestación de servicios.
Las personas o grupos de personas sobre las cuales se obtienen los datos	Servidores Públicos y aspirantes a ocupar un cargo dentro del Ayuntamiento de Etzatlán.
Procedimiento de recolección:	
Se les pide documentación referente a su Currículum Vitae, Comprobante de Domicilio, Identificación, formando un expediente para cada trabajador y/o servidor público. Para la selección del personal, se le da vista al presidente municipal para la aprobación de su contratación.	
Tipo de soporte en donde se contienen los datos personales	Formatos físicos y electrónicos.
Características del lugar de resguardo	En las oficinas del área generadora de la información.

Estructura básica del sistema y la descripción de los tipos de datos incluidos	
Datos generales del sistema	
Responsable	Titular en turno
Domicilio	Escobedo No. 320. Colonia Centro. C.P. 46500 Etzatlán , Jalisco
Teléfono	01 (386) 7530026 Ext. 104
Correo electrónico	oficialiamayor@etzatlan.gob.mx
Administradores	Oficial Mayor Administrativo, y Auxiliar
Domicilio	Escobedo No. 320. Colonia Centro. C.P. 46500 Etzatlán , Jalisco
Teléfono	01 (386) 7530026 Ext. 104
Datos personales incluidos en el sistema / inventario	
Tipo de datos personales	Nombre, edad, sexo, fecha de nacimiento, lugar de nacimiento, domicilio particular, correo electrónico personal, teléfonos particulares, credencial electoral, documentos oficiales que acrediten su personalidad, estado civil, firma particular, fotografía, CURP, datos del RFC.
Tipo de tratamiento	Tratamiento no automatizado y automatizado. El que requiera el trámite, siempre y cuando sea lícito, conforme a las nuevas medidas de seguridad.
Cesión de las que puede ser objeto la información confidencial	
Las medidas que establezca de conformidad a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.	

Unidades internas, sujetos obligados, autoridades o terceros a los que en su caso se ceden los datos.	No se transfiere información a ninguna autoridad o sujeto obligado, salvo orden emitida por autoridad competente.
Finalidad	
Nivel de protección exigible	
Básico	
Medio	
Alto	X
Normatividad:	
Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.	

Seguimiento a juicios	
Datos de identificación	
Unidad Administrativa Responsable	Jefatura Jurídica
Contenido del sistema	
Finalidad de sistemas y los usos previstos	Dar seguimiento a los juicios de los cuales el municipio es parte de ellos, como dar contestación a oficios, amparos y juicios de nulidad.
Las personas o grupos de personas sobre las cuales se obtienen los datos	Servidores públicos del Ayuntamiento de Etzatlán
Procedimiento de recolección	La recolección se realiza de forma presencial en dicha Dirección.
Tipo de soporte en donde se contienen los datos personales	Formatos físicos y electrónicos.

Características del lugar de resguardo	Archivos electrónicos.
Estructura básica del sistema y la descripción de los tipos de datos incluidos	
Datos generales del sistema	
Área	Jefatura de Jurídico
Responsable	Titular en turno
Domicilio	Escobedo No. 320. Colonia Centro. C.P. 46500 Etzatlán , Jalisco
Teléfono	01 (386) 7530026 Ext.
Correo electrónico	juridico@etzatlan.gob.mx
Administradores	Titular de Jefatura en Turno, y Auxiliar
Datos personales incluidos en el sistema / inventario	
Tipo de datos personales	Nombre, Edad, Teléfono
Tipo de tratamiento	Tratamiento no automatizado y automatizado.
sesión de las que puede ser objeto la información confidencial	Las medidas que establezca de conformidad a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.
Unidades internas, sujetos obligados, autoridades o terceros a los que en su caso se ceden los datos.	

Ninguno	
Finalidad	Dar seguimiento a los juicios de los cuales el municipio es parte de ellos, como dar contestación a oficios, amparos y juicios de nulidad.
Nivel de protección exigible	
Básico	
Medio	X
Alto	
Fundamentación	Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

Asuntos de seguridad pública, detenidos, armamento y siniestro	
Datos de identificación	
Sujeto Obligado	Municipio de Etzatlán
Unidad Administrativa Responsable	Comisaría de Seguridad Pública
Contenido del sistema	
Finalidad de sistemas y los usos previstos	Registro de datos de personas detenidas por la policía municipal.
Las personas o grupos de personas sobre las cuales se obtienen los datos	Detenidos y policías municipales
Procedimiento de recolección	La recolección se realiza de forma presencial en dicha Dirección.
Tipo de soporte en donde se contienen los datos personales	Formatos físicos y electrónicos.
Características del lugar de resguardo	Archivos electrónicos.
Estructura básica del sistema y la descripción de los tipos de datos incluidos	
Datos generales del sistema	
Área	Comisaría de Seguridad Pública

Responsable	Comisario de Seguridad Pública en turno
Domicilio	Escobedo No. 320. Colonia Centro. C.P. 46500 Etzatlán , Jalisco
Teléfono	01 (386) 7530083
Correo electrónico	seguridad@etzatlan.gob.mx
Administradores	Comisario de seguridad pública y auxiliar
Datos personales incluidos en el sistema / inventario	
Tipo de datos personales	Nombre, edad, fecha de nacimiento, estado civil, nacionalidad, origen étnico, CURP , RFC, fotografías personales, información familiar, información de sus hijos (nombre, edad, estado de salud y/o discapacidad), información laboral, domicilio particular, número de teléfono particular, correo electrónico particular, estado civil, firma, datos socioeconómicos, estado de salud (enfermedades y/o discapacidades).
Tipo de tratamiento	Tratamiento no automatizado y automatizado.
Cesión de las que puede ser objeto la información confidencial	
Unidades internas, sujetos obligados, autoridades o terceros a los que en su caso se ceden los datos.	No se transfiere ninguna información, salvo orden oficial emitida por autoridad competente.
Finalidad	Medio probatorio para la persecución de delitos.

Nivel de protección exigible	
Básico	
Medio	
Alto	X
Normatividad:	
Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.	

Denuncia ciudadana	
Datos de identificación	
Sujeto Obligado	Municipio de Etzatlán
Unidad Administrativa Responsable	Comisaría de Seguridad Pública
Contenido del sistema	
Finalidad de sistemas y los usos previstos	Registro de reportes ciudadanos
Las personas o grupos de personas sobre las cuales se obtienen los datos	Cualquier ciudadano que hace el reporte
Procedimiento de recolección	La recolección se realiza de forma presencial en dicha Dirección.
Tipo de soporte en donde se contienen los datos personales	Formatos físicos y electrónicos.
Características del lugar de resguardo	Archivos electrónicos.
Estructura básica del sistema y la descripción de los tipos de datos incluidos	
Datos generales del sistema	

Responsable	Comisario de seguridad pública en turno
Domicilio	Escobedo No. 320. Colonia Centro. C.P. 46500 Etzatlán , Jalisco
Teléfono	01 (386) 7530083
Correo electrónico	seguridad@etzatlan.gob.mx
Administradores	Comisario de seguridad pública, y Auxiliar
Datos personales incluidos en el sistema / inventario	
Tipo de datos personales	Nombre, edad, fecha de nacimiento, estado civil, nacionalidad, origen étnico, CURP , RFC, fotografías personales, información familiar, información de sus hijos (nombre, edad, estado de salud y/o discapacidad), información laboral, domicilio particular, número de teléfono particular, correo electrónico particular, estado civil, firma, datos socioeconómicos, estado de salud (enfermedades y/o discapacidades).
Tipo de tratamiento	Tratamiento no automatizado y automatizado.
Cesión de las que puede ser objeto la información confidencial	
Unidades internas, sujetos obligados, autoridades o terceros a los que en su caso se ceden los datos.	No se transfiere ninguna información, salvo orden oficial emitida por autoridad competente.
Finalidad	Medio probatorio para la persecución de delitos.

Nivel de protección exigible	
Básico	
Medio	
Alto	X
Normatividad:	
Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.	

DEBERES DE LOS SERVIDORES PÚBLICOS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

Para garantizar la aplicación correcta de este sistema es necesario establecer los deberes de los servidores públicos del municipio que participan en el tratamiento de los datos personales derivado de sus atribuciones.

Al momento de recibir los datos personales el servidor público que se encargue de su recepción deberá:

1. Tener a la vista el Aviso de Privacidad.
2. Dar a conocer el aviso de privacidad al titular de los datos personales antes de la obtención de sus datos.
3. En caso de dudas y/o quejas de los titulares de los datos personales sobre el tratamiento de sus datos, orientar al ciudadano para que acuda a la Dirección de Transparencia.
4. Al obtener los datos personales cerciorarse de que la información esté completa, sea veraz y comprensible.
5. Comunicar discrepancias de los datos personales recabados a su jefe inmediato o al administrador de los datos personales.
6. Conocer y seguir las medidas de seguridad que le sean aplicables para el cuidado de los datos personales, durante el periodo en el que posea los datos personales.
7. Recabar los datos personales para la finalidad para la cual estos fueron recabados según el trámite o el sistema de tratamiento que corresponda.
8. Tratar los datos personales de manera lícita siguiendo los principios establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco.

9. Conocer, aplicar y sujetarse al Aviso de Privacidad y al Documento de Seguridad del Gobierno Municipal de Etzatlán, en el tratamiento de datos personales.
10. Guardar estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones.

El servidor público involucrado en el *tratamiento de datos personales* deberá:

1) Conocer, aplicar y sujetarse al Aviso de Privacidad y al Documento de Seguridad del Gobierno Municipal de Etzatlán, en el tratamiento de datos personales.

2) Aplicar las medidas de seguridad correspondientes a los datos personales tratados y/o el sistema de protección en el que participa.

3) Tratar los datos personales de manera lícita siguiendo los principios establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco.

4) En caso de dudas o quejas de los titulares de los datos personales sobre el tratamiento de sus datos, orientar al ciudadano para que acuda a la Dirección de Transparencia.

5) Guardar estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones.

6) Abstenerse de realizar transferencias de datos personales que no vayan de conformidad con la finalidad para la cual se obtuvieron los datos.

El servidor público que *administra los datos personales* deberá:

1. Conocer, aplicar y sujetarse al Aviso de Privacidad y al Documento de Seguridad del Gobierno Municipal de Etzatlán, en el tratamiento de datos personales.
2. Aplicar nuevas medidas de seguridad que resulten accesibles y viables para la protección de datos personales.
3. Tratar los datos personales para la finalidad para la cual estos fueron recabados según el trámite o el sistema de tratamiento que corresponda.
4. Tratar los datos personales de manera lícita siguiendo los principios establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco.
5. Guardar estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones.
6. En caso de dudas o quejas de los titulares de los datos personales sobre el tratamiento de sus datos, orientar al ciudadano para que acuda a la Dirección de Transparencia.
7. Informar a la Dirección de Transparencia sobre los cambios que sufran sus trámites o sistemas de tratamiento de datos personales, los riesgos y las vulneraciones que surjan en el tratamiento de los datos personales, las medidas

Son obligaciones del Comité de Transparencia en relación al tratamiento de datos personales, además de las previstas en el artículo 87 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco:

1) Revisar anualmente las políticas y/o lineamientos en materia de protección de datos personales establecidos en el presente documento.

2) Emitir o aprobar anualmente un programa de capacitaciones en materia de protección de datos personales.

3) Requerir anualmente a las dependencias o áreas responsables que tratan datos personales a través de la Dirección de Transparencia, informes sobre el tratamiento de los datos personales y la aplicación de medidas de seguridad, así como vulneraciones detectadas en el año.

Son obligaciones de la Dirección de Transparencia en relación al tratamiento de datos personales, además de las previstas en el artículo 88 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco:

1) Difundir al interior del Gobierno Municipal de Etzatlán el aviso de privacidad y el documento de seguridad.

2) Revisión física anual a 5 dependencias sobre el tratamiento de datos personales y la implementación de medidas de seguridad.

3) Proponer al Comité de Transparencia actualizaciones o modificaciones al documento de seguridad.

4) Emitir un reporte anual al Comité de Transparencia sobre el ejercicio de estas funciones.

El Órgano de Control Interno , conforme a sus atribuciones establecidas en el artículo 89 del Reglamento Interior del Gobierno y de la Administración Pública del Municipio de Etzatlán, Jalisco, podrá hacer revisiones o auditorías sobre la aplicación del presente documento de seguridad.

ANÁLISIS DE RIESGO:

Debido a las circunstancias generales, tanto físicas como humanas, en las que se tratan datos personales, hemos logrado identificar los siguientes riesgos posibles ante los que se pudiera enfrentar este Sujeto Obligado:

- Obtención de datos incompletos o incorrectos.
- Omitir la notificación al titular de los datos personales del aviso de privacidad.
- No difundir el aviso de privacidad.
- El titular de los datos personales no conoce los términos del aviso de privacidad.
- No tener un lugar seguro y de acceso restringido en donde se puedan archivar los datos personales en físico.
- Permitir a todo servidor público o personas ajenas a la dependencia, el acceso a los expedientes que contienen datos personales.
- Pérdida de expedientes físicos debido a catástrofes, inundaciones, e incendios.
- Daño de la base de datos que contenga información confidencial.
- Fallas en los equipos de cómputo en donde se encuentran las bases de datos.
- Falta de capacitación de los servidores públicos en relación a la confidencialidad que deben guardar sobre los datos personales que conozcan debido al desempeño de sus funciones.
- Pérdida, robo o extravío de expedientes.

- Alteración de la información.
- Hackeo de los equipos de cómputo.

Ante dichos riesgos identificados es necesario hacer un análisis de dichos riesgos, amenazas y sus posibles vulneraciones.

Origen de la amenaza:	**Causa:**	**Posibles consecuencias:**
Acceso de personas no autorizadas a los sistemas o plataformas oficiales del municipio.	Adquirir información o datos personales.	● Acceso no autorizado. ● Divulgación de datos personales. ● Robo de información. ● Modificaciones no autorizadas. ● Robo de información.
Acceso de personas no autorizadas como criminales o traficantes de datos a los sistemas o plataformas oficiales del municipio.	Adquirir datos personales para utilizarlos con fines de explotación, chantaje, extorsión o cualquier uso criminal.	● Extorsiones. ● Ataques a personas. ● Robo de información. ● Vulneración a la seguridad física y mental de los ciudadanos. ● Robo de información.
Personal del sujeto obligado con poco conocimiento sobre el tratamiento de datos personales.	● Poca preparación académica. ● Irresponsabilidad laboral. ● Desconocimiento de los procesos de recolección de datos.	● Obtener información para beneficio personal. ● Uso ilícito de datos personales. ● Error involuntario. ● Robo de información. ● Extorsión.

		● Modificaciones no autorizadas.
Daño físico.	● Agua. ● Fuego. ● Corrosión.	Daño o pérdida de los datos personales.
Eventos naturales.	● Desastres climatológicos. ● Sismos. ● Cualquier eventualidad por causa natural.	Daño o pérdida de los datos personales.
Fallas técnicas.	● Pérdida de electricidad. ● Falla o pérdida de internet. ● Falla en sistemas, correos electrónicos o plataformas oficiales.	● Daño o pérdida de los datos personales. ● Divulgación y transferencia de datos personales.
Decadencias técnicas.	● Mantenimiento insuficiente. ● Falla en equipos. ● Obsolencia de equipos de telecomunicaciones o cómputos.	Pérdida, destrucción y daño.
Susceptibilidad en redes o sistemas autorizados.	● Falta de contraseñas altamente efectivas. ● Falta de mecanismos para	● Pérdida, destrucción y daño. ● Divulgación y transferencia de datos personales. ● Modificaciones no autorizadas.

	autenticación de usuarios. ● Falta de actualización de antivirus.	● Robo de información.
Organización.	Procesos carentes de formalidad, administración, acceso, uso y proceso de archivo.	● Pérdida, destrucción y daño. ● Divulgación y transferencia de datos personales no autorizados. ● Modificaciones no autorizadas. ● Robo de información.
Espacio donde se archiven.	● Carencia de espacio. ● Espacio con poca seguridad. ● Espacio no adecuado.	● Daño o pérdida de los datos personales. ● Divulgación y transferencia de datos personales. ● Modificaciones no autorizadas. ● Robo de información.

ANÁLISIS DE BRECHA:

Una vez identificados los posibles riesgos a los que este Sujeto Obligado se encuentra susceptible, podemos realizar el análisis de brecha, en donde los enlaces reportaron las siguientes medidas de seguridad existentes:

- Quien recaba los datos personales, es un servidor público del área, asignado especialmente para recabar datos en general necesarios para cada trámite.
- El espacio físico o área donde se recaban datos personales, es dentro de las instalaciones municipales.
- Cuando los datos personales son recabados de forma digital, se realiza por medio de plataformas oficiales o correo electrónico oficial.
- En la mayoría de las áreas, el acceso se tiene restringido, una vez que el dato se encuentra en posesión del servidor público, es decir si fue recabado frente a un escritorio, ventanilla, área abierta o pasillo, los ciudadanos no podrán pasar detrás de estos, ya que al terminar de recabar datos estos se colocan fuera del alcance de los ciudadanos.
- Cada oficina cuenta con puertas que separan el área al momento de terminar labores.
- Las llaves que se tienen de cada área se encuentran en manos de servidores públicos, autorizados por cada área.
- Una vez recabados los datos personales, el servidor público genera un expediente para cada trámite o servicio, del cual se obtuvieron los datos personales, ya sea físico o electrónico.
- Una vez recabados los datos personales, ya realizada la carpeta o expediente (electrónica, física, en plataformas, o cualquiera generada) y guardada esta en archiveros o puesta en resguardo electrónico, tienen acceso a esta área servidores públicos del área.
- Las llaves de los archiveros con las que se cuentan se encuentran en posesión de servidores públicos encargados del área.
- Una vez recabados los datos personales, en caso de que se siga un proceso electrónico, el servidor público guarda los mismos en carpeta electrónica, ya sea en su computadora, carpeta compartida, correo electrónico oficial o plataforma.
- Durante el desahogo del trámite del cual se obtuvieron los datos personales, los servidores públicos del área tienen acceso a los datos personales.

- Una vez concluido el trámite, los datos personales recabados se dejan intactos en la carpeta, archivo o expediente del trámite al que pertenecen.
- Cada carpeta de trámites o archivo, al terminar el proceso de cada uno, son resguardados en un archivo de cada área.

Las medidas de seguridad que actualmente se llevan a cabo pudieran ser efectivas de aplicarse de manera continua y consciente en las áreas administrativas del sujeto obligado. El riesgo latente que se provoca por la falta de conocimiento, o compromiso para la aplicación de estas medidas existentes se puede minimizar por medio del establecimiento obligatorio de dichas medidas de seguridad y de la mejora continua de las mismas.

MEDIDAS DE SEGURIDAD:

Con base en lo anterior se establecen las siguientes medidas de seguridad de carácter físico, técnico y administrativo:

Objetivo de control	Descripción
Control de servidores públicos que recaban los datos personales.	Debe realizarse un listado de los servidores públicos que recaban datos personales, esto es, de los servidores públicos que tienen contacto con el titular de los datos personales por sus funciones. Actualización del listado: cada 6 meses.
Capacitación de servidores públicos que recaban los datos personales.	Forzosa asistencia a por lo menos a 1 capacitación en materia de datos personales.

Responsabilidad de servidores públicos que recaban los datos personales.	Remitir el documento de seguridad para el conocimiento y cumplimiento de las medidas de seguridad aplicables para un correcto tratamiento de datos personales.
Obtención de datos.	Para evitar el riesgo de obtener datos personales incompletos o incorrectos, el servidor público autorizado para recabarlos, deberá pedir al ciudadano acredite su personalidad.
Aviso de privacidad.	El servidor público que reciba los datos personales, deberá tener a la vista de todos los ciudadanos el aviso de privacidad, y darlo a conocer al momento de la recepción del trámite.
Aviso de privacidad.	Si el trámite del cual se recabarán datos personales, cuenta con un formato, este deberá contener la mención y debe dar a conocer el aviso de privacidad del municipio, ya sea simplificado o la liga de internet que remita al ciudadano al aviso general. Los formatos nuevos que se impriman posteriores a la emisiòn del presente documento deberán contar con la liga al aviso de privacidad o en su defecto el aviso de privacidad simplificado.
Aviso de privacidad	Si el trámite del cual se recabarán datos personales, fue recabado mediante una plataforma electrónica oficial, esta plataforma deberá contener la mención y debe dar a conocer el aviso de privacidad del municipio, ya sea simplificado o la liga de internet que remita al ciudadano al aviso general.
Correcta obtención de datos	Los datos personales recabados deberán ser recibidos únicamente en las instalaciones de cada

personales.	área.
Espacio físico seguro	El área específica donde se recaben los datos deberá contar con puertas que tengan llave, sin excepción alguna, para asegurar de forma efectiva el trato adecuado de los datos personales, así evitar mal uso de los mismos o vulneraciones.
Espacio físico seguro	Las llaves de las puertas de cada dependencia, deberán ser guardadas únicamente por servidores públicos del área, autorizados para poseer las llaves.
Espacio físico seguro	Al término de las labores, deberá cerrarse cada oficina de las áreas, para evitar el contacto de otros servidores públicos o ciudadanos con los datos personales recabados.
Espacio físico seguro	Al concluir la jornada laboral, se deberá guardar los expedientes, para no dejarlos al alcance de ciudadanos o personal no autorizado.
Resguardo provisional, durante el desahogo del trámite	Una vez recabados los datos personales, al generar el expediente (derivado del trámite), este deberá ponerse en algún lugar que esté fuera del alcance de los ciudadanos, ya sea en una caja, archivero, o mueble.
Archivo, al finalizar el desahogo del trámite	Al finalizar el desahogo de los expedientes estos deberán archivarse en un lugar adecuado con las siguientes características: ● No estar al alcance de los ciudadanos o servidores públicos ajenos al área. ● Deberá ser un área específica para guardar los expedientes. Este archivo debe estar bajo

	llave. ● La llave del mismo solo puede estar en manos de un servidor
Acceso al archivo.	Se deberá crear por cada área, un control o bitácora de los servidores públicos que tienen acceso al archivo, el control debe contener lo siguiente: ● Registro para anotar el nombre y puesto del servidor público autorizado. ● Firma de conformidad del servidor público que entró. ● Firma de consentimiento del servidor público autorizado para llevar el control de este archivo. ● Fecha, hora de entrada y hora de salida del archivo. ● Registrar el expediente que se consultó. ● Registrar el expediente que se extrae del archivo y la fecha.
Control de archivos electrónicos.	Cuando los datos personales sean recabados por medios electrónicos, se deberá generar expediente por cada trámite, dicho expediente deberá ser guardado en base de datos, correo electrónico oficial, o en plataforma autorizada, no en cualquier plataforma o correo electrónico personal.
Control de archivos electrónicos.	Para evitar riesgos, respecto a los expedientes electrónicos, se debe contar con un respaldo electrónico. Dicho respaldo deberá realizarse, como mínimo, de manera anual.
Inventarios Documentales sobre archivos entregados a la Dirección de Archivos.	Cada área del sujeto obligado deberá elaborar controles de archivo, conforme a sus procesos institucionales. Esto es, un inventario de documentos que se mandan a la Dirección de Archivo para su resguardo en el Archivo Municipal.

Transferencia de datos personales.	En caso de ser necesario derivado de las funciones de los servidores públicos, o por requisito del trámite, se deba realizar una transferencia de datos personales, se deberá informar al sujeto que reciba los datos el aviso de privacidad para que se sujete al mismo.
Versiones Públicas	En los casos en los cuales se realicen clasificaciones de información confidencial, que incluyan datos personales, los documentos que contengan los datos, deberán entregarse siempre en versión pública, adjuntando índice de datos personales.
Archivo finalizado	Al momento de finalizar el trámite, todos los expedientes, deberán desecharse y enviarse y mandarse al archivo municipal, conforme a la normatividad correspondiente.

Medidas de seguridad para transferencias:

Transferencias al interior del sujeto obligado y a otros sujetos obligados:

- Solo podrán ser transferidos los datos personales para dar seguimiento y conclusión al trámite o sistema de tratamiento bajo la finalidad que éstos prevean.
- El área que entrega los datos personales deberá cerciorarse de transferir la totalidad de los datos que resulten necesarios para el seguimiento o la conclusión del trámite o sistema de tratamiento correspondiente, limitándose la entrega de datos adicionales que no resulten necesarios.
- El área que entrega los datos personales deberá cerciorarse de que los datos que transfiere sean completos y veraces.
- El área que reciba los datos personales deberá conservar los mismos sujetándose a las finalidades y lineamientos del aviso de privacidad de este sujeto obligado y adoptando las medidas de seguridad previstas en este documento.

- El área que reciba los datos personales deberá encargarse de la supresión de los datos que reciba cuando esta corresponda.
- El área que entrega y el área que recibe los datos personales deberán dar acceso a los datos personales en tratándose de procedimientos de derecho ARCO.

Transferencias a terceros:

- El tercero que reciba los datos personales deberà sujetarse a las finalidades y lineamientos del aviso de privacidad de este sujeto obligado y deberá adoptar las medidas de seguridad previstas en este documento.
- En caso de ser necesario conforme a las disposiciones normativas, se deberá firmar un convenio o acuerdo de confidencialidad que proteja el tratamiento de los datos personales que recaba este sujeto obligado y transfiere al tercero.

Medidas de seguridad en caso de vulneraciones a la seguridad:

En caso de ocurrir alguna vulneración deberá registrarse en la bitácora de contingencias, misma que deberá seguirse bajo el siguiente formato:

Fecha en la que ocurrió	Motivo	Las acciones correctivas implementadas de forma inmediata y definitiva

Después del registro, se deberá informar de forma inmediata al titular y a la Unidad de Transparencia las vulneraciones de seguridad ocurridas, las que afecten o impacten de forma significativa los derechos patrimoniales o morales del titular, en un plazo máximo de setenta y

dos horas en cuanto se confirmen y este en proceso las acciones encaminadas para dimensionar la afectación, con la finalidad de que los titulares puedan tomar medidas correspondientes para la defensa de sus derechos, dicha notificación debe contener lo siguiente:

I. La naturaleza del incidente.

II. Los datos personales comprometidos.

III. Las recomendaciones y medidas que el titular puede adoptar para proteger sus intereses.

IV. Las acciones correctivas realizadas de forma inmediata.

V. Los medios donde puede obtener mayor información al respecto.

Al ocurrir una vulneración de seguridad, el servidor público titular del área responsable y/o el responsable del sistema deberá analizar la causa por lo que ocurrió dicha vulneración, e implementar y anexar a su plan de trabajo las acciones preventivas y correctivas para adecuar medidas de seguridad que prevengan esta eventualidad, para evitar que la vulneración se repita.

A su vez, en caso de detectar que la falla fue ocasionada por el incumplimiento de un servidor público a su cargo deberá levantar acta circunstanciada de hechos correspondiente y seguir el procedimiento administrativo correspondiente ante la Contraloría Municipal.

Medidas de seguridad o controles para la identificación y autenticación de los usuarios:

Parte de tener control efectivo al trato de los datos personales es contar con un sistema que garantice la autenticación de usuarios, esto es por medio de administración de cuentas creadas específicamente para cada servidor público.

La administración de cuentas de usuario es una parte esencial de los sistemas que se desarrollan en el departamento de software. La razón principal de las cuentas de usuario es verificar la identidad de cada funcionario, también permite la utilización personalizada de acceso a la información y generación de la misma.

Esta medida es tomada para los correos electrónicos institucionales y para cualquier sistema o plataforma tecnológica que cree este sujeto obligado.

El estándar para la creación de las cuentas es:

- ❏ Usuario: Generalmente es el correo electrónico institucional
- ❏ Contraseña: Frase de confirmación de identidad que se encuentra encriptada para mayor seguridad.

Estos accesos son dados, por parte de la Dirección de Innovación del Gobierno Municipal de Guadalajara, mediante una carta responsiva personalizada la cual va firmada por el interesado y la persona que autoriza.

Medidas de seguridad para la supresión y borrado seguro de datos personales:

De conformidad con el artículo 3 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios fracción V, el bloqueo se dará únicamente después del cumplimiento de la finalidad con la que fueron recabados los datos personales hasta que cumpla el plazo de prescripción legal o contractual correspondiente, concluido éste se deberá proceder a la supresión en la base de datos, archivo, registro, expediente que corresponda, al mismo tiempo se está garantizando la supresión de los datos personales.

Ahora bien especificaremos los objetivos de contar con técnicas apropiadas para la supresión y borrado de datos personales:

- ➔ Que la supresión y borrado de los expedientes que contengan datos personales sea de forma legal.
- ➔ Que la supresión y borrado de los expedientes que contengan datos personales sea de forma operativa conforme a los procedimientos utilizados en el municipio.
- ➔ Servir como base para el proceso adecuado de supresión y borrado de los expedientes que contengan datos personales.
- ➔ Guía para depuración de datos personales.

Bases para supresión y borrado seguro de archivos:

- ★ Las bajas documentales se realizan mediante la aprobación del pleno del Ayuntamiento y a solicitud del área encargada de su resguardo.
- ★ Los documentos físicos cuya baja ha sido procedente, se entregan a un reciclador.
- ★ De acuerdo a la Ley que Regula la Administración de los Documentos Públicos e Históricos del Estado de Jalisco, los documentos dados de baja cuentan con una antigüedad mayor a los 10 (diez) años, y ya no cuentan con ningún tipo de vigencia ni validez alguna.

Plan de contingencia:

Ante la pérdida total o parcial de datos personales en posesión de este sujeto obligado, se debe contar con un plan de contingencia.

Con la evaluación de riesgos y la elaboración de las medidas de seguridad aplicables para prevenir las posibles vulneraciones a las que nos encontramos expuestos, el plan de contingencias de este sujeto obligado consiste en la aplicación de las medidas de seguridad tratadas en el apartado anterior, mismas que están sujetas a cambios por eventualidades no contempladas, por ello la importancia de señalar que el presente se trata de un plan de contingencia no limitativo.

En caso de que los datos personales sufran algún tipo de daño o pérdida, se dispondrá de los respaldos electrónicos realizados por cada área administrativa en donde se contienen copias de documentos y/o archivos y/o bases de datos que contienen datos personales que permitirían restablecer los datos a la fecha del último respaldo.

Plan de trabajo:

La existencia del documento de seguridad, busca enmarcar los deberes del Municipio de Etzatlán para la máxima protección de datos personales. Debido a la importancia y el contexto actual en materia de datos personales, se debe mantener actualizado el plan de trabajo, el cual permita alcanzar los objetivos del sistema de seguridad de protección de datos personales.

La finalidad de este plan es plasmar de manera enunciativa, más no limitativa, las actividades que el Municipio de Etzatlán realizará para la aplicación del presente documento de seguridad.

Lo anterior se realizará en base a las atribuciones establecidas en el la Ley de Protección de Datos Personales en Posesión de sujetos Obligados del Estado de Jalisco y sus Municipios.

Para la ejecución del presente documento de seguridad, al inicio de cada año:

1. Se emitirá circular para difundir la emisión del presente documento, a través de la cual se remitirá copia digital del mismo a todos los correos institucionales vigentes.
2. Se comunicará a los enlaces sobre la emisión del documento de seguridad, solicitando su apoyo para la difusión interna del mismo.
3. Se buscará la participación del ITEI para una primera capacitación básica para los servidores públicos que recaban datos personales.

El Comité de Transparencia, de manera anual, a partir de la emisión del presente documento de seguridad:

1. Revisará lo concerniente al índice de Datos Personales y mantenerlo actualizado.
2. Actualizará las medidas de seguridad conforme al Sistema de Protección de Datos Personales hecho para el Municipio de Etzatlán.
3. Actualizará el plan de trabajo.
4. Emitirá un programa anual de capacitaciones y además se promoverá que el personal del Municipio se mantenga capacitado no sólo por sus áreas internas, sino también mediante su asistencia a capacitaciones otorgadas por organismos competentes en la materia.

Mecanismos de monitoreo y revisión de las medidas de seguridad:

Se debe realizar un monitoreo y revisión de la aplicación de las medidas de seguridad, para valorar las amenazas, vulnerabilidades, aplicación correcta o incorrecta, impacto y actualización. Esto con el objetivo de que las medidas de seguridad continúen siendo efectivas e idóneas para el municipio.

En el siguiente cuadro se concentran los mecanismos de monitoreo y el objetivo de cada uno de ellos:

Mecanismos de monitoreo.	**Objetivo del monitoreo.**
Visitas a 3 áreas cada 12 meses, las áreas serán elegidas de forma aleatoria.	Verificar de primera mano la aplicación, actualización e impacto de las medidas de seguridad aplicadas.
Pedir reportes a los responsables de cada área generadora de información o a los responsables del sistema de datos personales o a sus administradores sobre el manejo de datos personales conforme a las medidas de seguridad.	Monitorear y monitorear avances, aplicación, eventualidades y novedades respecto a la aplicación de las medidas de seguridad.

Programa general de capacitación:

Se manejarán las capacitaciones de conformidad con las necesidades del sujeto obligado en cuanto a la implementación y aplicación del sistema de manejo de datos personales, en posesión del sujeto obligado.

Las fechas exactas se les notificarán a los Enlaces de Transparencia con al menos una semana de anticipación a las fechas estimadas con la intención de que éstos las difundan con los interesados en asistir a las capacitaciones.

POLÍTICAS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES:

Las políticas de privacidad en materia de protección de datos personales pueden ser consultadas en nuestro sitio oficial a través de la siguiente dirección electrónica: https://etzatlan.gob.mx/adpt/