DOCUMENTO DE SEGURIDAD
UNIDAD DE TRANSPARENCIA
MAZAMITLA, JALISCO
2024-2027

I. Introducción

Con el avance exponencial que han tenido en los últimos años sistemas tales como el Gobierno Abierto, la Transparencia, la Rendición de Cuentas o la Protección de Datos Personales, emparejado al crecimiento y perfeccionamiento de los organismos encargados de custodiar el cumplimiento de las obligaciones que se derivan de tales conceptos, tenemos plena conciencia en la Unidad de Transparencia (UT) del Gobierno de Mazamitla de que la información es un activo que debe protegerse mediante un conjunto de procesos y sistemas diseñados, administrados y mantenidos por la propia UT. De esta manera, la gestión de la seguridad de la información, como parte de un sistema transparente 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 Unidad puede afrontar.

El presente Documento de Seguridad, 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. Al mismo tiempo, servirá como una guía que permitirá brindar homogeneidad en la organización, procesos y sistemas, en donde el Comité de Transparencia, conjuntamente con las áreas del sujeto obligado y los responsables de los sistemas de datos personales, definen las medidas de seguridad administrativa y física implementadas para la protección de los sistemas de datos

personales custodiados. En conclusión, este documento tiene como propósito controlar internamente el universo de sistemas de datos personales que posee la Unidad, el tipo de datos personales que contiene, los responsables, encargados, usuarios de cada sistema y las medidas de seguridad concretas implementadas.

En la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios se establecen las bases, principios, procedimientos y tratamiento que permite garantizar la protección de datos personales de los ciudadanos en posesión del municipio como sujeto obligado.
Teniendo como base dicha normatividad, y de conformidad con sus artículos 3 fracción XIV, artículo 30 al 44 y a la Guía para Implementar un Sistema de Gestión de Seguridad de Datos Personales del 2015, emitida por el entonces Instituto Federal de Acceso a la Información, la cual puede ser consultada en la siguiente liga http://inicio.ifai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf, se crea el presente documento de seguridad.

OBJETIVOS –

Describir el proceso que lleva a cabo la Unidad de Transparencia y Acceso a la Información Pública del Municipio, para garantizar la seguridad física y el cumplimiento de las normas comprendidas en la materia, atendiendo a las especificaciones de la guía para la elaboración de un documento de seguridad emitida por el IFAI y la elaboración de especificaciones, guías, procedimientos generales, instrucciones de trabajo y registros de control propios.

- Describir y dar 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.

MARCO JURÍDICO

a) Constitución Política de los Estados Unidos Mexicanos.

b) Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

c) Lineamientos de Protección de Datos Personales. Emitidos por el Instituto Federal de Acceso a la Información Pública.

d) Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.

e) Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

ÁMBITO DE APLICACIÓN

El presente Documento de Seguridad es aplicable y de observancia obligatoria para la Unidad de Transparencia del Municipio de Mazamitla, Jalisco, en cumplimiento a las funciones que le son inherentes, así como para las personas externas que, debido a la presentación de un servicio, tengan acceso a tales sistemas o al sitio donde se ubican los mismos.

DISPOSICIONES GENERALES

1.- TIPOS DE MEDIDAS DE SEGURIDAD

Las medidas de seguridad deben implementarse para la obtención de los objetivos contemplados en los siguientes propósitos:
a) Política de seguridad. Definición de normas estratégicas en materia de seguridad de activos, alineadas a las atribuciones del Gobierno de Mazamitla, Jalisco. Incluye la elaboración y emisión interna de expedientes.
b) Cumplimiento de la normatividad. Los controles establecidos para evitar violaciones de la normatividad vigente, obligaciones contractuales o la política de seguridad interna. Abarca, entre otros, la identificación y el cumplimiento de requerimientos tales como la legislación aplicable, los derechos de propiedad intelectual, la protección de datos personales y la privacidad de la información personal.
c) Organización de la seguridad de la información. Establecimiento de controles internos y externos a través de los cuales se gestione la seguridad de activos. Considera, entre otros aspectos, la organización interna, que a su vez se refiere al compromiso de la alta dirección y la designación de responsables, entre otros objetivos; asimismo, considera aspectos externos como la identificación de riesgos relacionados con terceros
d) Administración de incidentes. Implementación de controles enfocados a la gestión de incidentes presentes y futuros que puedan afectar la integridad, confidencialidad y disponibilidad de la información. Incluye temas tales como debilidades de seguridad de la información.
e) Continuidad de las operaciones. Establecimiento de medidas con el fin de contrarrestar las interrupciones graves de la operación y fallas mayores en los sistemas de información. Incluye planeación, implementación, prueba y mejora del plan de continuidad de la operación del sujeto obligado.

2.- NIVELES DE PROTECCIÓN DE LOS DATOS PERSONALES

Las medidas de seguridad que son aplicables a la Unidad de Transparencia del Municipio de Mazamitla, Jalisco, deberán considerar el tipo de datos personales que contiene, lo cual determina el nivel de protección requerido, siendo básico o alto, como a continuación se establece:
a) Nivel de protección básico: Datos de identificación. - Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad nombres de familiares, dependientes y beneficiarios, fotografía, costumbres, idioma o lengua entre otros.
b) Nivel de protección Alto: ▪ Datos ideológicos: creencia religiosa, ideología, afiliación política y/o sindical, perteneciente a organizaciones de la sociedad civil y asociaciones religiosas, entre otros. ▪ Características personales: Tipo de sangre, ADN, huella dactilar u otros análogos. ▪ Características físicas: Color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros. ▪ Vida sexual: Preferencia sexual, hábitos sexuales, entre otros. ▪ Origen: Étnico y racial. ▪ La Unidad de Transparencia, a través de las solicitudes presentadas, debe asegurar de acuerdo con la

naturaleza de los datos contenidos en los sistemas de datos personales que custodia, los niveles de protección conforme a su grado de confidencialidad, disponibilidad e integridad.

3.- TIPO DE TRANSMISIONES DE DATOS PERSONALES Y MODALIDADES PARA LA TRANSMISIÓN.

Se deberán considerar el tipo de transmisión que se pueden llevar a cabo dependiendo de quién sea el destinatario:

a. Intermunicipales. A cualquier municipio que sea necesario derivar una solicitud, presentada ante la Unidad que no sea de su jurisdicción, y que sea dentro de los 125 municipios del Estado de Jalisco.

b. Traslado electrónico: En esta modalidad se transmiten al destinatario los datos personales en archivos electrónicos contenidos en medios de almacenamiento inteligibles sólo mediante el uso de algún correo electrónico que procese su contenido para examinar, modificar o almacenar los datos.

El presente documento se guiará por los principios, y conceptos que establece Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

II. De las funciones y obligaciones de las personas que tratan 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 derivados 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 previo a la obtención de sus datos.
3) 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 UT.
4) Al obtener los datos personales cerciorarse de que la información esté completa, actualizada, sea veraz, y comprensible.
5) Comunicar discrepancias de los datos personales recabados a su jefe inmediato o al administrador de los datos personales, ello cuando se dé cuenta.
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 Mazamitla, en el tratamiento de datos personales.
10) Guardar estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones.
11) Tomar, una vez al año un curso, taller o capacitación sobre el tratamiento de

datos personales.
12) Sujetarse a lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco.

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 Mazamitla, 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 UT.
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.
7) Tomar, una vez al año, un curso, taller o capacitación sobre el tratamiento de datos personales.
8) Sujetarse a lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco.

El servidor público que administra los datos personales, conforme los sistemas de tratamiento vigente deberá:
1) Conocer, aplicar y sujetarse al Aviso de Privacidad y al Documento de Seguridad del Gobierno Municipal de Mazamitla, en el tratamiento de datos personales.
2) Conocer e implementar las medidas de seguridad establecidas en el documento de seguridad.
3) Aplicar nuevas medidas de seguridad que resulten accesibles y viables para la protección de datos personales.
4) Supervisar a los servidores públicos que participan en la recepción y en el tratamiento de datos personales en cada trámite o sistema.
5) Tratar los datos personales para la finalidad para la cual estos fueron recabados según el trámite o el sistema de tratamiento que corresponda.
6) 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.
7) Guardar estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones.
8) Tomar, una vez al año, un curso, taller o capacitación sobre el tratamiento de datos personales.
9) Informar a los titulares de los datos sobre nuevas finalidades del tratamiento de datos personales o nuevas transferencias.
10) 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 UT.
11) Informar a la UT 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 correctivas implementadas y las transferencias nuevas que realicen de los datos personales.
12) Acudir a la UT en caso de asesoría sobre el tratamiento de datos personales.
13) Monitorear de manera cotidiana la implementación de las medidas de seguridad y levantar actas circunstanciadas de hechos ante la reincidencia de un incumplimiento en la aplicación de las mismas.
14) Dar aviso al Comité de Transparencia, a través de la UT, sobre las actas circunstanciadas de hechos levantadas por el incumplimiento del documento de seguridad y sobre el seguimiento de las mismas.
15) Sujetarse a lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco.

El servidor público responsable de cada sistema, o en su caso, el titular de la Unidad Administrativa responsable de cada sistema deberá:
1) Conocer, aplicar y sujetarse al Aviso de Privacidad y al Documento de Seguridad del Gobierno Municipal de Mazamitla, en el tratamiento de datos personales.
2) Implementar las medidas de seguridad que establece el documento de seguridad.
3) Guardar estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones.
4) Tomar una vez al año un curso, taller o capacitación sobre el tratamiento de datos personales.
5) 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 UT.
6) Aplicar medidas correctivas en caso de identificar incidentes, alteraciones o vulneraciones en el tratamiento de datos personales.
7) Informar a la UT 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 correctivas implementadas y las transferencias nuevas que realicen de los datos personales.
8) Monitorear la implementación de las medidas de seguridad.
9) Monitorear de manera cotidiana la implementación de las medidas de seguridad y levantar actas circunstanciadas de hechos ante la reincidencia de un incumplimiento en la aplicación de las mismas.
10) Dar aviso al Comité de Transparencia, a través de la UT, sobre las actas circunstanciadas de hechos levantadas por el incumplimiento del documento de seguridad y sobre el seguimiento de las mismas.
11) Presentar propuestas de mejora o modificación del documento de seguridad a través de la UT.
12) Emitir reportes en relación al tratamiento de los datos personales y la aplicación de medidas de seguridad, según sea requerido por el Comité de Transparencia a través de la Dirección de Transparencia.
13) Diseñar, desarrollar e implementar políticas públicas, procesos internos, y/o sistemas o plataformas tecnológicas necesarias para el ejercicio de sus funciones apegándose en todo momento al documento de seguridad, las políticas o lineamientos que para el tratamiento de datos personales emita el Comité de Transparencia, la UT y el ITEI, así como a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco.
14) Sujetarse a lo establecido en la Ley de Protección de Datos Personales en Posesión

de Sujetos Obligados del Estado de Jalisco.

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 el aviso de privacidad y el documento de seguridad.
2) Revisión física anual a 2 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.

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 UT, informes sobre el tratamiento de los datos personales y la aplicación de medidas de seguridad, así como vulneraciones detectadas en el año.

La Contraloría del Gobierno Municipal de Mazamitla, conforme sus atribuciones, podrá hacer revisiones o auditorías sobre la aplicación del presente documento de seguridad.

III. Del análisis de riesgos

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.
● Ante la necesidad de tener un consentimiento expreso: no tener evidencia de que el titular de los datos personales 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.

Ante dichos riesgos identificados es necesario hacer un análisis de dichos riesgos, amenazas y sus posibles vulneraciones.
Hasta el momento no se han identificado o reportado vulneraciones desde las áreas generadoras de información o las dependencias que integran el Gobierno Municipal de Mazamitla.

IV. Del análisis de brecha
Una vez identificados los posibles riesgos a los que este Sujeto Obligado se encuentra susceptible de enfrentar, podemos realizar el análisis de brecha, utilizando como base las entrevistas que se hicieron con cada enlace que tiene la UT con diferentes áreas del Gobierno Municipal.

Las áreas administrativas 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.
● 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 (al área donde se recibe a los ciudadanos y se recaban datos personales) 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 separa 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 está 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 les dé 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.

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 a 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 deberá 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.

Después del registro, se deberá informar de forma inmediata al titular y al instituto 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 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.

Bases para supresión y borrado seguro de archivos:
· Las bajas documentales se realizan mediante la aprobación del pleno del Ayuntamiento.
· Los documentos físicos cuya baja ha sido procedente, se entregan a un reciclador.
Los documentos son vigilados por personal del Gobierno Municipal hasta su destino final, en donde son triturados.
· 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.

V. Del 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, nos encontramos con que 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.

Lo anterior toda vez que en la actualidad existen cambios y grandes avances que van modificando la organización de la información, y al igual existan riesgos inminentes que día a día evolucionan. Con la aplicación de las medidas de seguridad establecidas en este documento se buscan minimizar los riesgos o vulneraciones, pero a su vez se intenta propiciar el restablecimiento de los datos personales en el menor tiempo posible ante cualquier eventualidad.
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.

VI. Los 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 continúan siendo efectivas e idóneas para el municipio.

ARTÍCULO TRANSITORIO

PRIMERO. El presente apartado normativo del Documento de Seguridad entrará en vigor al día siguiente de su aprobación por el Comité de Transparencia.

SEGUNDO: El presente Documento de Seguridad deberá ser publicado en el portal de transparencia municipal, Artículo 8, Fracción I) Inciso a).

Amanda Albarrán R.

AMANDA ALBARRAM RAMOS	**LIC. LIZBETH CEJA CHAVEZ**
Presidente Municipal	Unidad de Transparencia