COMISIÓN ESTATAL DEL AGUA DE JALISCO

DOCUMENTO DE SEGURIDAD

COMITÉ DE TRANSPARENCIA

El presente documento contiene las disposiciones en materia de protección de datos personales de las unidades administrativas que forman parte de esta Comisión Estatal del Agua de Jalisco.

2019

Documento de Seguridad de la Comisión Estatal del Agua de Jalisco

Contenido

- **Aprobación del Documento de Seguridad por parte del Comité de Transparencia**

Introducción

La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios tiene por objeto establecer las bases, principios, obligaciones y procedimientos para garantizar el derecho que tiene toda persona al debido tratamiento y protección de sus datos personales. Así como a garantizar el derecho de acceso, rectificación, cancelación y oposición de los mismos.

Teniendo como base la normativa de esta Ley y de conformidad con su artículo 3 fracción XIV y los artículos contenidos dentro del Título Segundo Capítulo II (art 30 al 44); así como la Guía para Implementar un Sistema de Gestión de Seguridad de Datos Personales del 2015, emitida por el Instituto Nacional del Transparencia y Protección de Datos Personales Federal de Acceso a la Información; al igual que la Guía para elaborar un Documento de Seguridad/Formato guía para sujetos obligados del año 2018.

A partir de la publicación de la Ley, la Comisión Estatal del Agua de Jalisco por conducto del titular de su Unidad de Transparencia, con la participación de los enlaces de transparencia de las Unidades Administrativas generadoras de información, se establecieron las acciones conducentes con la finalidad de establecer los soportes para la realización del presente documento.

Una de las acciones primordiales fue la elaboración de un Inventario de Datos Personales que permite la identificación básica de información y el tratamiento al que son sometidos por cada una de las Unidades Administrativas y sensibilizar a estas sobre la importancia del resguardo de datos personales.

El presente documento permite identificar los datos personales recabados por esta CEA y en consecuencia la creación del Sistema de Tratamiento de Datos Personales sobre los mismos.

Desde la publicación de la multicitada Ley, la Unidad de Transparencia de la CEA ha realizado capacitaciones especializadas en materia de protección de datos personales con la finalidad de enseñar, habilitar e instruir a los servidores públicos sobre el tratamiento lícito y adecuado de los datos personales.

Para la realización del Inventario de Datos Personales, por medio de los enlaces de transparencia se realizó un cuestionario en la materia de cada una de sus áreas a todas las Unidades Administrativas; mediante este estudio se detectaron los datos personales recabadas por cada una de ellas, así como las medidas de seguridad con las que se contaban dentro de la CEA e identificar los posibles riesgos.

A partir de la creación del Inventario de Datos Personales, capacitaciones y diversas sesiones con los enlaces de transparencia, se recabó la información necesaria para generar cada una de las partes que integran el presente Documento de Seguridad; en donde el objetivo primordial es la protección y adecuado tratamiento de los datos personales custodiados por esta CEA.

El Documento de Seguridad que se leerá a continuación se rige por los principios que marca la Ley, primordialmente por lo dictado en su numeral 2.

Objetivo

Este documento es de orden obligatorio y su objetivo es asegurar la integridad, la confidencialidad y disponibilidad de los datos e información personal que se encuentran en posesión de la Comisión Estatal del Agua de Jalisco, en su carácter de Sujeto Obligado. Del mismo modo delimita las obligaciones de los responsables, encargados y usuarios de cada sistema y medidas de seguridad administrativa, física y técnica que deberán implementarse para el correcto manejo de la información que se posee. Lo anterior de conformidad a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, así como lo establecido en la Ley de Transparencia y Acceso a la Información del Estado de Jalisco y sus Municipios y su Reglamento.

El presente Documento de Seguridad fue elaborado por la Unidad de Transparencia y aprobado en su totalidad por el Comité de Transparencia, ambos de este sujeto obligado, mismo que será de observancia obligatoria para todos los servidores públicos de este organismo público descentralizado, así como para todas las personas externas que debido a la prestación de algún servicio deba tener acceso a la información, sistema o sitio web en el que se ubique cualquier tipo de dato personal protegido por esta CEA.

Sobre el Documento de Seguridad.

El presente documento se refiere al instrumento que describe y da cuenta de manera general sobre las medidas de seguridad, técnicas, físicas y administrativas que ha adoptado la Comisión Estatal del Agua de Jalisco, para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que se encuentran en posesión de esta sujeto obligado.

De los Datos Personales

Los datos personales, así como la información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de información tal como nombre, domicilio, número de teléfono, número de seguridad social, datos relativos al patrimonio, las que se refieran a sus características físicas, morales o emocionales, a su vida familiar, entre otros.

Los Datos Personales Sensibles son aquellos que se refieren a la esfera íntima de su titular, o cuya utilización indebida puede dar origen a discriminación o conlleve un riesgo grave para éste. Tales como los relativos a su origen étnico o racial, estado de salud, información genética, datos biométricos, creencias religiosas, filosóficas y morales, opiniones políticas y preferencias sexuales u otros similares.[1]

Este Organismo Público Descentralizado deberá regirse y actuar bajo los principios enunciados en la Ley, como lo es la licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad.

[1] Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, artículo 3 fracciones IX y X

Sobre el Aviso de Privacidad

Si los ciudadanos o instituciones privadas proporcionan a la Comisión Estatal del Agua de Jalisco información confidencial, esta deberá de dar a conocer las políticas respecto de su protección, de conformidad con lo señalado por la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado del Jalisco y sus Municipios y los Lineamientos que establezca el Instituto de Transparencia Acceso a la Información Pública y Protección de Datos Personales del Estado de Jalisco. El Aviso de Privacidad especifica las medidas que ha tomado la Comisión Estatal del Agua de Jalisco para garantizar la seguridad en el tratamiento de los datos personales que se recaban con motivo de trámites o del desempeño propio de las labores de este sujeto obligado, a través del cual se evita su alteración, pérdida, transmisión, publicación y acceso no autorizado.

Sobre los Derechos ARCO

Se trata de solicitudes sobre los datos personales que posee el sujeto obligado sobre los cuales se ejerce el derecho al Acceso, Rectificación, Cancelación y Oposición de los mismos, las cuales podrá realizar solamente el titular de los datos personales o su representante legal.

Es de vital importancia hacer incapié que para cualquier trámite relacionado al ejercicio de los Derechos ARCO, por razones de seguridad y protección de los datos personales que este sujeto obligado posee, debe ser demostrada la identificación plena del solicitante, a través de los medios legales establecidos para ellos (credencial INE, pasaporte vigente, cédula profesional, cartilla militar) tanto para solicitar la información como para recibirla.

La única instancia facultada dentro de la Comisión Estatal del Agua para el tratamiento de los Datos Personales, es el Comité de Transparencia, mismo que entrará al estudio y evaluará la procedencia de las solicitudes de Derechos Arco de conformidad con la normativa estatal vigente, así como en base a los lineamientos dispuestos por el Instituto de Transparencia Acceso a la Información Pública y Protección de Datos Personales del Estado de Jalisco. El Comité de Transparencia deberá realizar una resolución debidamente fundada y motivada, la que será notificada al solicitante, respecto de la solicitud de cualquiera de los Derechos ARCO.

El Tratamiento de la Información por parte de los Sujetos Obligados

Los sujetos obligados deberán adoptar las medidas necesarias para el debido tratamiento, manejo, mantenimiento, seguridad y protección de la información confidencial que obre en su poder, así como los procedimientos necesarios para garantizar la protección, tratamiento, mantenimiento, seguridad sobre el destino final de los datos personales que posean con motivo de sus atribuciones.

El tratamiento de datos personales, debe versar sobre toda aquella información que pueda encontrarse en cualquier material, ya sea en documento o medios digitales, como fotografías, grabaciones, soporte magnético, digital, sonoro, visual, electrónico, informático u otro elemento análogo.

De los Responsables y Encargados de la Protección de los Datos Personales e Información Confidencial

Solo podrán tener acceso a la información confidencial en posesión de este sujeto obligado, los miembros del Comité de Transparencia, el titular de la Unidad de Transparencia, los titulares de las Unidades Administrativas y/o los usuarios quienes por las labores que desempeñan, deberán de tener acceso a dicha información. Los anteriormente mencionados serán los responsables de resguardarla, así como promover las medidas necesarias para su tratamiento y custodia.

Por su parte el Comité de Transparencia, con ayuda de la Unidad de Transparencia, se encargará de establecer la información que tenga carácter de confidencial o reservada.

- Dictará las medidas necesarias para el tratamiento que deba darse a los datos personales en términos de las disposiciones legales aplicables, entendiendo en todo momento y como política institucional que estos tienen el carácter de reservada, salvo que se dicte disposición contraria por la autoridad competente para el caso concreto o que quien solicite la información sea el titular de la misma.

Medidas de Seguridad

Se trata de todas aquellas medidas que adopta el Comité de Transparencia de la Comisión Estatal del Agua de Jalisco y en su caso, en conjunto con el área que los posea, siempre que sea necesario para asegurar que la información confidencial y los datos personales sean resguardados, de manera íntegra, segura y adecuada, ya sea a través de mecanismos administrativos, técnicos, físicos, políticas de procesos y controles.

De conformidad con lo señalado por la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco, los deberes sobre la Seguridad de los datos personales, se entenderán tal y como lo marca el artículo 30 que a la letra dice:

*"**Artículo 30.** Deberes — Seguridad de los datos personales.*
1. Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad; sin perjuicio de lo establecido por las disposiciones vigentes en materia de seguridad emitidas por las autoridades competentes al sector que corresponda, cuando éstas contemplen una protección mayor para el titular o complementen lo dispuesto en esta Ley y demás disposiciones aplicables."

Dentro de las medidas de seguridad que se tienen señaladas por la Ley y que deben ser seguidos los elementos que ahí se señalan, se encuentran:

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. De manera enunciativa más no limitativa, se debe considerar las siguientes actividades:*

a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico, que pueda salir fuera de las instalaciones de la organización; y
d) Proveer a los equipos que contienen o almacena datos personales de un mantenimiento eficaz que asegure su disponibilidad, funcionalidad e integridad.

Medidas de seguridad técnicas: *Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con harware y software para proteger el entorno digital de los datos personales y recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:*

a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados.
b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware; y
d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales[2]

[2] Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, artículo 3, fracción XXV, XXVI, XXVII y XXVIII.

Con lo anterior se pretende que únicamente personal autorizado y plenamente identificado tenga acceso a los datos personales en posesión de este sujeto obligado y, así también, que el servidor público que tenga acceso a dicha información evite que ésta sea divulgada, a efecto de no comprometer la integridad, confiabilidad y disponibilidad de los sistemas de datos.

Objetivo de la Implementación de Medidas de Seguridad sobre los Datos Personales

Es atribución del Comité de Transparencia de la CEA establecer las recomendaciones sobre las políticas de manejo, mantenimiento, seguridad y protección de datos personales, que estén en posesión de las unidades administrativas de este organismo público descentralizado, así como identificar aquellos datos que se recaban y posee, las responsables, las encargadas y usuarios de cada sistema interno con los que se cuenta y las medidas de seguridad concretas implementadas por este sujeto obligado.

Por lo que es necesario promover la adopción de las medidas de índole técnica y organizativa necesarias para garantizar la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

Para lograrlo se deben tomar en cuenta los avances tecnológicos, la naturaleza de los datos almacenados y los riesgos a que puedan estar expuestos, si provienen de la acción humana o de las condiciones físicas y ambientales, por lo que se han establecido distintos niveles de seguridad aplicables a cada categoría o tipo de datos alojados en los sistemas de datos personales.

Los alcances que deben de tener las recomendaciones son para convertirse en propuestas y sugerencias específicas para lograr la mayor protección de datos personales, por lo que las unidades administrativas de la CEA podrán utilizarlas como modelo a seguir y así tener la forma de seguridad sin perjuicio de que establezcan medidas adicionales que coadyuven a la mejor protección, la integridad, confidencialidad y disponibilidad de la información persona que se tiene.

El documento deberá mantenerse siempre actualizado y ser de observancia obligatoria para todos los servidores públicos de esta CEA, así como para las personas externas que debido a la prestación de un servicio tengan acceso a determinado sistema o al sitio donde se ubican los mismos.

De los Niveles de Seguridad

En cuanto a los niveles de seguridad que se deben tomar respecto de la información que se posee, es necesario aclarar que los mismos no se encuentran establecidos en la legislación vigente, no obstante es de gran importancia que esta CEA, establezca como políticas mínimas de actuación, aquellas contempladas en los estándares más altos y de mayor uso, y que sean tomadas como base para el tratamiento y resguardo de los datos personales con los que contamos.

En ese sentido, para este caso particular, tomaremos como referencia, el estándar internacional ISO/IEC 27002:2005, referente a las practicas sobre seguridad de información y que son tomadas a su vez como ejemplo por el Instituto Nacional de Transparencia en sus Recomendaciones sobre Medidas de Seguridad Aplicables a los Sistemas de Datos Personales.

Lo anterior a fin de garantizar la protección de datos personales que tengan en posesión, estableciendo personal autorizado para la protección y promover el uso responsable de las nuevas tecnologías de la información, atendiendo los principios de protección de datos.

Por lo que tomando en cuenta los criterios establecidos sobre medidas de seguridad, para el resguardo eficaz de los datos personales, al final de cada medida, se establecen niveles de seguridad, las cuales deberán observarse atendiendo a la naturaleza de la información contenida en los sistemas establecidos.

Por lo tanto, las áreas que integran la CEA aplicarán el nivel básico, medio o alto de medidas de seguridad, de acuerdo con la categoría o tipos de datos personales.

1. NIVEL BÁSICO.-

Estas medidas serán aplicables a todos los sistemas de datos personales[3]

- ***De Identificación:*** *Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma (en cuanto ésta no resulta confidencial cuando se emita en cumplimiento de la obligación legal para las funciones que fue contratado el servidor público y deba autorizar la emisión de un documento que por sus actividades resulta necesario para avalar el contenido del texto), 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.*

- ***Labores:*** *Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio*

[3] Recomendaciones sobre Medidas de Seguridad Aplicables a los Sistemas de Datos Personales https://www.gob.mx/cms/uploads/attachment/file/83122/MODELOS_Y_GU_AS_17-pdf

de trabajo, correo electrónico institucional (contraseña e información de procesos administrativos de la bandeja de entrada), actividades extracurriculares, referencias laborales, referencias personales entre otros.

La posesión de datos personales deberá obedecer exclusivamente a las atribuciones legales o reglamentarias de cada entidad y deberán obtenerse a través de los medios previstos, estos datos sólo deberán tratarse únicamente para la finalidad para la cual fueron obtenidos.

Cuando los datos personales se actualicen no deben de alterar la veracidad de la información que tengan y debe de ser por personal autorizado para el cumplimiento de las atribuciones de esta CEA.

2. NIVEL MEDIO.-

Los datos personales además de cumplir con las medidas de seguridad de nivel básico, deberán observar las marcadas en el nivel medio[4]

- ***Datos Patrimoniales:*** *Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros.*

- ***Datos sobre procedimientos administrativos seguidos en forma de juicio y/o jurisdiccionales:*** *Información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa.*

- ***Datos Académicos:*** *Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros.*

[4] IBID página 14

- ***Tránsito y movimientos migratorios:*** *Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas entre otros.*

Este tipo de datos debido a la trascendencia para la intimidad, se debe evitar prejuicios por el uso que se pueda hacer con ese tipo de información siendo factores de generar graves conflictos, si no tienen el debido cuidado al manejar la información confidencial.

3. NIVEL ALTO.-

Los datos personales que contengan algún dato que se enliste deberán cumplir con las medidas de seguridad de nivel básico y medio, deberán observar las marcadas con el nivel alto.

- ***Datos Ideológicos:*** *Creencia religiosa, ideología, filosófica, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y/o asociaciones religiosas, entre otros.*

- ***Datos de Salud:*** *Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, entre otros.*

- ***La ubicación de menores de edad:*** *a través de sus datos académicos y toda la información que se posea de estos, toda vez que la revelación de algún dato personal puede poner en riesgo la integridad de menores.*

- ***Características personales:*** *Tipo de sangre, ADN, huella digital, u otros análogos.*

- ***Características físicas:*** *Color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otras.*

- ***Vida sexual:*** *Preferencia sexual, hábitos sexuales, entre otros.*

- ***Origen:*** *Étnico y racial.*

Los niveles de protección señalados definen el mayor o menor grado de confidencialidad, disponibilidad e integridad que el sujeto obligado debe asegurar de acuerdo con la naturaleza de los datos personales que custodia, de conformidad con las siguientes definiciones:

*La **confidencialidad** es asegurar que la información no sea accedida por – o divulgada a- personas o procesos no autorizados.*

*La **integridad** es garantizar la exactitud y la confiabilidad de la información y los sistemas de manera que éstos no puedan ser modificados sin autorización, ya sea accidental o intencionalmente.*

*La **disponibilidad** es que las personas o procesos autorizados accedan a los activos de información cuando así lo requieran*[5]

[5] Recomendaciones sobre Medidas de Seguridad Aplicables a los Sistemas de Datos Personales. http://www.gob.mx/cms/uploads/attachment/file/83122/MODELOS_Y_GU_AS_17.pdf

Accesos Controlados y Bitácoras

Deberá guardarse como mínimo los datos completos del responsable, encargado o usuario, el modo de autenticación del Responsable, encargado o usuario, fecha y hora en se realizó el acceso, o se intentó el mismo sistema de datos personales accedido, operaciones o acciones llevadas a cabo dentro del sistema de datos personales, fecha y hora en que se realizó la salida del sistema de datos personales.[6]

Operaciones de Acceso, Actualización, Respaldo y Recuperación.

Se debe de contar con manuales de procedimientos y funciones para el tratamiento de datos personales que deberán observar obligatoriamente los Responsables, encargados o usuarios de los sistemas de datos personales.[7]

Llevar control y registros del sistema de datos personales en bitácoras que contengan la operación cotidiana, respaldos, usuarios, incidentes y accesos, así como la transmisión de datos y sus destinatarios, de acuerdo con las políticas internas que establezca la entidad.

Procedimientos de control de acceso a la red que incluyan perfiles de usuarios o grupos de usuarios para el acceso restringido a las funciones y programas de los sistemas de los datos personales.

Deberán contar con mecanismos de auditoría o rastreabilidad de operaciones y así garantizar que el personal encargado del tratamiento de datos personales sólo tenga acceso a las funciones autorizadas del sistema de datos personales según su perfil de usuario. Aplicar procedimientos de respaldo de base de datos y realizar pruebas periódicas de restauración, se tendrá que llevar el control de

[6] GUIA PARA LA ELABORACIÓN DE UN DOCUMENTO DE SEGURIDAD V 1.4

[7] IBID

inventarios y clasificación de los medios magnéticos u ópticos de respaldo de los datos personales.

Utilizar un espacio externo seguro para guardar de manera sistemática los respaldos de base de datos personales y el transporte de los sistemas de datos personales, se debe garantizar que, durante la transmisión de datos personales y el transporte de los soportes de almacenamiento, que no se pueda tener acceso a los datos, que no sean, reproducidos, alterados o suprimidos sin autorización.

La aplicación de los procedimientos para la destrucción de medios de almacenamiento y de respaldo obsoletos que contengan datos personales. En los casos en que la operación sea externa, convenir con el responsable de cada unidad administrativa que tenga la facultad de verificar que se respete la integridad, confiabilidad, confidencialidad y disponibilidad de los datos personales, revisar que el tratamiento se está realizando conforme a lo establecido.

Diseñar planes de contingencia que garanticen la continuidad de la operación y realizar pruebas de eficiencia de los mismos.

Llevar a cabo las verificaciones a través de las áreas de tecnología de la información, informática o su equivalente y cualquier otra medida tendente a garantizar el cumplimiento de los principios de protección de datos personales.[8]

[8] IBID

SISTEMAS DE SEGURIDAD, IDENTIFICACIÓN Y NIVELES DE SEGURIDAD POR UNIDAD ADMINISTRATIVA A TRAVÉS DEL ORGANIGRAMA DE LA COMISIÓN ESTATAL DEL AGUA DE JALISCO.

DIRECCIÓN ÁREA DE CUENCAS Y CULTURA DEL AGUA

DATOS DE IDENTIFICACIÓN			
	Día	Mes	Año
Fecha de Elaboración	08	06	2019
Sujeto Obligado	Comisión Estatal del Agua de Jalisco		
Unidad Administrativa Responsable	Dirección de Área de Cuencas y Cultura del Agua		
CONTENIDO DEL SISTEMA			
Finalidad de sistemas y los usos previstos	Capacitación hacia los responsables de cultura de los Municipios del estado. Obtención de datos personales derivado de los cursos impartidos por el personal de cultura del agua de esta CEA.		
Personas o grupos de personas sobre las cuales se obtienen los datos	Ciudadanos que reciben dicho curso.		
Procedimiento de recolección	Listados en formatos físicos.		
Tipo de soporte en donde se contienen los datos personales	ELIMINADO. Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Su publicación pondría en riesgo a la Comisión pues reflejaría las posibles vulnerabilidades de soportes de contenidos de datos personales y sus lugares de resguardo.		
Características del lugar de resguardo			
ESTRUCTURA BÁSICA DEL SISTEMA Y LA DESCRIPCIÓN DE LOS TIPOS DE DATOS INCLUIDOS			
DATOS GENERALES DEL SISTEMA			
Área	Responsable	Cargo	
Dirección de Área de Cuencas y Cultura del Agua	Ing. Armando Brigido Muñoz Juárez	Director de Área de Cuencas y Cultura del Agua	

ADMINISTRADORES		
Área	Administrador	Cargo
Dirección de Área de Cuencas y Cultura del Agua	Carmen Julia Rodríguez Covarrubias	Promotor
Dirección de Área de Cuencas y Cultura del Agua	Luis Alberto Rodríguez Macías	Promotor
Dirección de Área de Cuencas y Cultura del Agua	Ileana Marcela Cota Contreras	Promotor

DATOS PERSONALES INCLUIDOS EN EL SISTEMA/INVENTARIO	
TIPO DE DATOS PERSONALES	
Nombre, Teléfono particular, Correo electrónico	
Tipo de Tratamiento	Tratamiento no automatizado y automatizado. El que sea requerido, siempre y cuando sea lícito, conforme a las nuevas medidas de seguridad.

TRANSFERENCIA DE LA QUE PUEDE SER OBJETO LA INFORMACIÓN CONFIDENCIAL		
Los datos obtenidos no son transferibles		Los datos obtenidos no son transferibles
Nivel de protección exigible.	x	Básico
		Medio
		Alto

FUNDAMENTACIÓN
Art. 3, fracción IX de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

DIRECCIÓN DE ÁREA CREACIÓN Y FORTALECIMIENTO DE ORGANISMOS OPERADORES

DATOS DE IDENTIFICACIÓN			
	Día	Mes	Año
Fecha de Elaboración	08	06	2019
Sujeto Obligado	Comisión Estatal del Agua de Jalisco		
Unidad Administrativa Responsable	Dirección de Área Creación y Fortalecimiento de Organismos Operadores		
CONTENIDO DEL SISTEMA			
Finalidad de sistemas y los usos previstos	Se recaban datos dentro de las Actas de los Consejos de Administración y Comisiones Tarifarias		
Personas o grupos de personas sobre las cuales se obtienen los datos	Ciudadanos representantes de los diferentes sectores		
Procedimiento de recolección	Se recaban dentro de las Actas		
Tipo de soporte en donde se contienen los datos personales	ELIMINADO. Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Su publicación pondría en riesgo a la Comisión pues reflejaría las posibles vulnerabilidades de soportes de contenidos de datos personales y sus lugares de resguardo.		
Características del lugar de resguardo			
ESTRUCTURA BÁSICA DEL SISTEMA Y LA DESCRIPCIÓN DE LOS TIPOS DE DATOS INCLUIDOS			
DATOS GENERALES DEL SISTEMA			
Área	Responsable	Cargo	
Dirección de Área Creación y Fortalecimiento de Organismos Operadores	Lic. Alejandro Alcázar Pellicer	Director de Área Creación y Fortalecimiento de Organismos Operadores	

ADMINISTRADORES		
Área	Administrador	Cargo
Dirección de Área Creación y Fortalecimiento de Organismos Operadores	Lic. José Saúl Ayala Carvajal	Jefe de Consolidación Financiera de los Servicios
Dirección de Área Creación y Fortalecimiento de Organismos Operadores	Lic. Claudia Olvera Escobedo	Jefe de Constitución de Organismos Operadores
Dirección de Área Creación y Fortalecimiento de Organismos Operadores	Lic. Daniel López Vázquez	Analista Administrativo

DATOS PERSONALES INCLUIDOS EN EL SISTEMA/INVENTARIO		
TIPO DE DATOS PERSONALES		
Nombre, Teléfono particular, Correo electrónico		
Tipo de Tratamiento	Tratamiento no automatizado y automatizado. El que sea requerido, siempre y cuando sea lícito, conforme a las nuevas medidas de seguridad.	
TRANSFERENCIA DE LA QUE PUEDE SER OBJETO LA INFORMACIÓN CONFIDENCIAL		
Organismos Operadores, Municipios y/o Dependencias Federales		Control de actos Jurídicos del Órgano Máximo de un organismo operador
Nivel de protección exigible.	X	Básico
		Medio
		Alto
FUNDAMENTACIÓN		
Art. 3, fracción IX de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.		

DIRECCIÓN DE ÁREA SOCIALIZACIÓN Y CONTRALORÍA SOCIAL

DATOS DE IDENTIFICACIÓN			
Fecha de Elaboración	Día 08	Mes 06	Año 2019
Sujeto Obligado	Comisión Estatal del Agua de Jalisco		
Unidad Administrativa Responsable	Dirección de Área Socialización y Contraloría Social		
CONTENIDO DEL SISTEMA			
Finalidad de sistemas y los usos previstos	Construcción de los Comités de Contraloría Social de la Función Pública. Censo de beneficiarios Actas de Comité		
Personas o grupos de personas sobre las cuales se obtienen los datos	Ciudadanos representantes de los diferentes sectores. Ciudadanos beneficiarios.		
Procedimiento de recolección	Listado en formato físico		
Tipo de soporte en donde se contienen los datos personales	ELIMINADO. Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Su publicación pondría en riesgo a la Comisión pues reflejaría las posibles vulnerabilidades de soportes de contenidos de datos personales y sus lugares de resguardo.		
Características del lugar de resguardo			
ESTRUCTURA BÁSICA DEL SISTEMA Y LA DESCRIPCIÓN DE LOS TIPOS DE DATOS INCLUIDOS			
DATOS GENERALES DEL SISTEMA			
Área	Responsable	Cargo	
Dirección de Área Socialización y Contraloría Social	Lic. José Enrique Pelayo	Director de Área Socialización y Contraloría Social	

ADMINISTRADORES		
Área	Administrador	Cargo

Dirección de Área Socialización y Contraloría Social	Rodolfo Enrique Montaño Gómez	Trabajador Social
Dirección de Área Socialización y Contraloría Social	María de los Ángeles González Casillas	Trabajador Social
Dirección de Área Socialización y Contraloría Social	Cristhian Arteaga García	Trabajador Social
Dirección de Área Socialización y Contraloría Social	Alejandro Martínez Díaz	Trabajador Social
Dirección de Área Socialización y Contraloría Social	Helios Alexander Santillán Valencia	Trabajador Social
Dirección de Área Socialización y Contraloría Social	Ariel Joseph Montoya García	Trabajador Social
Dirección de Área Socialización y Contraloría Social	Eliseo Ávila Pérez	Trabajador Social
Dirección de Área Socialización y Contraloría Social	Sergio Campos Romero	Trabajador Social
Dirección de Área Socialización y Contraloría Social	Fernando Oroz Vitar	Trabajador Social
Dirección de Área Socialización y Contraloría Social	Roberto Maldonado Vega	Trabajador Social
Dirección de Área Socialización y Contraloría Social	Alfonso Navarro Martín del Campo	Trabajador Social
DATOS PERSONALES INCLUIDOS EN EL SISTEMA/INVENTARIO		
TIPO DE DATOS PERSONALES		
Nombre, Teléfono particular, Correo electrónico		
Tipo de Tratamiento	Tratamiento no automatizado y automatizado. El que sea requerido, siempre y cuando sea lícito, conforme a las nuevas medidas de seguridad.	

TRANSFERENCIA DE LA QUE PUEDE SER OBJETO LA INFORMACIÓN CONFIDENCIAL		
Función Pública		Requisitos de los programas federales
Nivel de protección exigible.		Básico
	x	Medio
		Alto

FUNDAMENTACIÓN
Art. 3, fracción IX de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

DIRECCIÓN DE ÁREA VINCULACIÓN MUNICIPAL

DATOS DE IDENTIFICACIÓN			
Fecha de Elaboración	Día 08	Mes 06	Año 2019
Sujeto Obligado	Comisión Estatal del Agua de Jalisco		
Unidad Administrativa Responsable	Dirección de Área de Vinculación Municipal		
CONTENIDO DEL SISTEMA			
Finalidad de sistemas y los usos previstos	Obtención de Servidumbres de paso y/o sesión de predio necesarios para la ejecución de infraestructura hidráulica. Elaboración de Instrumentos Jurídicos.		
Personas o grupos de personas sobre las cuales se obtienen los datos	Ejidatarios y poseedores comuneros		
Procedimiento de recolección	Listado en formato físico/Censo		
Tipo de soporte en donde se contienen los datos personales	ELIMINADO. Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Su publicación pondría en riesgo a la Comisión pues reflejaría las posibles vulnerabilidades de soportes de contenidos de datos personales y sus lugares de resguardo.		
Características del lugar de resguardo			
ESTRUCTURA BÁSICA DEL SISTEMA Y LA DESCRIPCIÓN DE LOS TIPOS DE DATOS INCLUIDOS			
DATOS GENERALES DEL SISTEMA			
Área	Responsable	Cargo	
Dirección de Área Vinculación Municipal	María del Carmen Ramos	Director de Área Vinculación Municipal	

<table>
<tr><td colspan="3">ADMINISTRADORES</td></tr>
<tr><td>Área</td><td>Administrador</td><td>Cargo</td></tr>
<tr><td>Dirección de Área Vinculación Municipal</td><td>María de Jesús Ortega Mejía</td><td>Trabajador Social</td></tr>
<tr><td>Dirección de Área Vinculación Municipal</td><td>María del Rocío García Carrasco</td><td>Trabajador Social</td></tr>
<tr><td>Dirección de Área Vinculación Municipal</td><td>Pedro Hernández López</td><td>Jefe de Programas Federalizados</td></tr>
<tr><td>Dirección de Área Vinculación Municipal</td><td>Andrés Herrera Pérez</td><td>Analista de Estudios y Proyectos</td></tr>
<tr><td colspan="3">DATOS PERSONALES INCLUIDOS EN EL SISTEMA/INVENTARIO</td></tr>
<tr><td colspan="3">TIPO DE DATOS PERSONALES</td></tr>
<tr><td colspan="3">Nombre, Teléfono particular, Correo electrónico, INE</td></tr>
<tr><td>Tipo de Tratamiento</td><td colspan="2">Tratamiento no automatizado y automatizado. El que sea requerido, siempre y cuando sea lícito, conforme a las nuevas medidas de seguridad.</td></tr>
<tr><td colspan="3">TRANSFERENCIA DE LA QUE PUEDE SER OBJETO LA INFORMACIÓN CONFIDENCIAL</td></tr>
<tr><td colspan="2">No se transfieren</td><td>No se transfieren</td></tr>
<tr><td rowspan="3">Nivel de protección exigible.</td><td></td><td>Básico</td></tr>
<tr><td>X</td><td>Medio</td></tr>
<tr><td></td><td>Alto</td></tr>
<tr><td colspan="3">FUNDAMENTACIÓN</td></tr>
<tr><td colspan="3">Art. 3, fracción IX de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.</td></tr>
</table>

DIRECCIÓN ÁREA PLANTAS DE TRATAMIENTO DE AGUAS RESIDUALES

DATOS DE IDENTIFICACIÓN			
	Día	Mes	Año
Fecha de Elaboración	08	06	2019
Sujeto Obligado	Comisión Estatal del Agua de Jalisco		
Unidad Administrativa Responsable	Dirección de Área Plantas de Tratamiento de Aguas Residuales		
CONTENIDO DEL SISTEMA			
Finalidad de sistemas y los usos previstos	Administración y Padrón de usuarios del Parque Industrial El Salto		
Personas o grupos de personas sobre las cuales se obtienen los datos	Particulares que son usuarios del Parque Industrial El Salto		
Procedimiento de recolección	Listado en formato físico/Censo		
Tipo de soporte en donde se contienen los datos personales	ELIMINADO. Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Su publicación pondría en riesgo a la Comisión pues reflejaría las posibles vulnerabilidades de soportes de contenidos de datos personales y sus lugares de resguardo.		
Características del lugar de resguardo			
ESTRUCTURA BÁSICA DEL SISTEMA Y LA DESCRIPCIÓN DE LOS TIPOS DE DATOS INCLUIDOS			
DATOS GENERALES DEL SISTEMA			
Área	Responsable	Cargo	
Dirección de Área Plantas de Tratamiento de Aguas Residuales	Biol. Luis Aceves Martínez	Director de Área Plantas de Tratamiento de Aguas Residuales	

<table>
<tr><td colspan="4">ADMINISTRADORES</td></tr>
<tr><td>Área</td><td colspan="2">Administrador</td><td>Cargo</td></tr>
<tr><td>Dirección de Área Plantas de Tratamiento de Aguas Residuales</td><td colspan="2">Pablo Alejandro Jiménez Bautista</td><td>Jefe de Planta Potabilizadora El Salto</td></tr>
<tr><td colspan="4">DATOS PERSONALES INCLUIDOS EN EL SISTEMA/INVENTARIO</td></tr>
<tr><td colspan="4">TIPO DE DATOS PERSONALES</td></tr>
<tr><td colspan="4">Nombre, Teléfono particular, Domicilio, representante legal, Correo electrónico, INE, RFC, documentos oficiales que acrediten su personalidad</td></tr>
<tr><td>Tipo de Tratamiento</td><td colspan="3">Tratamiento no automatizado y automatizado. El que sea requerido, siempre y cuando sea lícito, conforme a las nuevas medidas de seguridad.</td></tr>
<tr><td colspan="4">TRANSFERENCIA DE LA QUE PUEDE SER OBJETO LA INFORMACIÓN CONFIDENCIAL</td></tr>
<tr><td colspan="2">No se transfieren</td><td colspan="2">No se transfieren</td></tr>
<tr><td rowspan="3">Nivel de protección exigible.</td><td></td><td colspan="2">Básico</td></tr>
<tr><td>X</td><td colspan="2">Medio</td></tr>
<tr><td></td><td colspan="2">Alto</td></tr>
<tr><td colspan="4">FUNDAMENTACIÓN</td></tr>
<tr><td colspan="4">Art. 3, fracción IX de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.</td></tr>
</table>

DIRECCIÓN DE ÁREA RECURSOS HUMANOS

DATOS DE IDENTIFICACIÓN			
Fecha de Elaboración	Día 08	Mes 06	Año 2019
Sujeto Obligado	Comisión Estatal del Agua de Jalisco		
Unidad Administrativa Responsable	Dirección de Área Recursos Humanos		
CONTENIDO DEL SISTEMA			
Finalidad de sistemas y los usos previstos	Conformación de Expedientes laborales y trámites administrativos que competen al trabajador		
Personas o grupos de personas sobre las cuales se obtienen los datos	Empleados de la Comisión Estatal del Agua de Jalisco		
Procedimiento de recolección	Recolección de documentos personales		
Tipo de soporte en donde se contienen los datos personales	ELIMINADO. Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Su publicación pondría en riesgo a la Comisión pues reflejaría las posibles vulnerabilidades de soportes de contenidos de datos personales y sus lugares de resguardo.		
Características del lugar de resguardo			
ESTRUCTURA BÁSICA DEL SISTEMA Y LA DESCRIPCIÓN DE LOS TIPOS DE DATOS INCLUIDOS			
DATOS GENERALES DEL SISTEMA			
Área	Responsable	Cargo	
Dirección de Área de Recursos Humanos	LAE. Luis Guillermo	Director de Área de Recursos Humanos	

<table>
<tr><td colspan="4">ADMINISTRADORES</td></tr>
<tr><td>Área</td><td colspan="2">Administrador</td><td>Cargo</td></tr>
<tr><td>Dirección de Área de Recursos Humanos</td><td colspan="2">Elizabeth Sahagún Jiménez</td><td>Jefe del Departamento de Control de Personal</td></tr>
<tr><td>Dirección de Área de Recursos Humanos</td><td colspan="2">Citlalli Maday García Gómez</td><td>Auxiliar Administrativo</td></tr>
<tr><td>Dirección de Área de Recursos Humanos</td><td colspan="2">René Pérez Chávez</td><td>Analista de Nómina</td></tr>
<tr><td colspan="4">DATOS PERSONALES INCLUIDOS EN EL SISTEMA/INVENTARIO</td></tr>
<tr><td colspan="4">TIPO DE DATOS PERSONALES</td></tr>
<tr><td colspan="4">Nombre, Teléfono particular, Domicilio, Correo electrónico, INE, RFC, CURP, Acta de Nacimiento, Certificado de Estudios, Comprobante de afiliación al IMSS, Cartilla de Servicio Militar (menores de 40 años), Fotografías, cartas de recomendación de particulares, Carta de No antecedentes penales, Examen médico, constancia de no sanción administrativa.</td></tr>
<tr><td>Tipo de Tratamiento</td><td colspan="3">Tratamiento no automatizado y automatizado. El que sea requerido, siempre y cuando sea lícito, conforme a las nuevas medidas de seguridad.</td></tr>
<tr><td colspan="4">TRANSFERENCIA DE LA QUE PUEDE SER OBJETO LA INFORMACIÓN CONFIDENCIAL</td></tr>
<tr><td colspan="2">No se transfieren</td><td colspan="2">No se transfieren</td></tr>
<tr><td rowspan="3">Nivel de protección exigible.</td><td></td><td colspan="2">Básico</td></tr>
<tr><td></td><td colspan="2">Medio</td></tr>
<tr><td>X</td><td colspan="2">Alto</td></tr>
<tr><td colspan="4">FUNDAMENTACIÓN</td></tr>
<tr><td colspan="4">Art. 3, fracción IX de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.</td></tr>
</table>

UNIDAD DE TRANSPARENCIA

DATOS DE IDENTIFICACIÓN			
	Día	Mes	Año
Fecha de Elaboración	08	06	2019
Sujeto Obligado	Comisión Estatal del Agua de Jalisco		
Unidad Administrativa Responsable	Dirección de Área de Jurídica		
CONTENIDO DEL SISTEMA			
Finalidad de sistemas y los usos previstos	Conformación de Expedientes de solicitudes de acceso a la información		
Personas o grupos de personas sobre las cuales se obtienen los datos	Ciudadanos que emiten solicitudes de acceso a la información.		
Procedimiento de recolección	Solicitudes recibidas por Plataforma Nacional de Transparencia, Oficialía de partes, correo electrónico, vía telefónica y remitidas por otras dependencias o entidades.		
Tipo de soporte en donde se contienen los datos personales	ELIMINADO. Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Su publicación pondría en riesgo a la Comisión pues reflejaría las posibles vulnerabilidades de soportes de contenidos de datos personales y sus lugares de resguardo.		
Características del lugar de resguardo			
ESTRUCTURA BÁSICA DEL SISTEMA Y LA DESCRIPCIÓN DE LOS TIPOS DE DATOS INCLUIDOS			
DATOS GENERALES DEL SISTEMA			
Área	Responsable	Cargo	
Dirección de Área Jurídica		Director de Área Jurídica	

	D. en D. Gelacio Juan Ramón Gutiérrez Ocegueda	

ADMINISTRADORES		
Área	Administrador	Cargo
Dirección de Área Jurídica	Lic. Laura Nayeli Pacheco Casillas	Titular de la Unidad de Transparencia
DATOS PERSONALES INCLUIDOS EN EL SISTEMA/INVENTARIO		
TIPO DE DATOS PERSONALES		
Nombre, Teléfono particular, Domicilio, Correo electrónico		
Tipo de Tratamiento	Tratamiento no automatizado y automatizado. El que sea requerido, siempre y cuando sea lícito, conforme a las nuevas medidas de seguridad.	
TRANSFERENCIA DE LA QUE PUEDE SER OBJETO LA INFORMACIÓN CONFIDENCIAL		
Unidades internas, sujetos obligados y/o autoridades que en su caso sea requerido ceder los datos		Finalidad
Nivel de protección exigible.	X	Básico
		Medio
		Alto
FUNDAMENTACIÓN		
Art. 3, fracción IX de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.		

DIRECCIÓN DE ÁREA FINANZAS

DATOS DE IDENTIFICACIÓN			
	Día	Mes	Año
Fecha de Elaboración	08	03	2019
Sujeto Obligado	Comisión Estatal del Agua de Jalisco		
Unidad Administrativa Responsable	Dirección de Área Finanzas		
CONTENIDO DEL SISTEMA			
Finalidad de sistemas y los usos previstos	Realizar los pagos por la transacción de servicios		
Personas o grupos de personas sobre las cuales se obtienen los datos	proveedores		
Procedimiento de recolección	Por medio de correo electrónico		
Tipo de soporte en donde se contienen los datos personales	ELIMINADO. Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Su publicación pondría en riesgo a la Comisión pues reflejaría las posibles vulnerabilidades de soportes de contenidos de datos personales y sus lugares de resguardo.		
Características del lugar de resguardo			
ESTRUCTURA BÁSICA DEL SISTEMA Y LA DESCRIPCIÓN DE LOS TIPOS DE DATOS INCLUIDOS			
DATOS GENERALES DEL SISTEMA			
Área	Responsable	Cargo	
Dirección de Área Finanzas	LCP. Juan Manuel García Díaz	Director de Área Finanzas	

ADMINISTRADORES		
Área	Administrador	Cargo

Dirección de Área Finanzas	Jorge Alberto Pérez Ureña	Jefe de Tesorería
DATOS PERSONALES INCLUIDOS EN EL SISTEMA/INVENTARIO		
TIPO DE DATOS PERSONALES		
Nombre y cuenta de clave interbancaria		
Tipo de Tratamiento	Tratamiento no automatizado y automatizado. El que sea requerido, siempre y cuando sea lícito, conforme a las nuevas medidas de seguridad.	
TRANSFERENCIA DE LA QUE PUEDE SER OBJETO LA INFORMACIÓN CONFIDENCIAL		
Los datos obtenidos no son transferibles		Los datos obtenidos no son transferibles
Nivel de protección exigible.		Básico
		Medio
	X	Alto
FUNDAMENTACIÓN		
Art. 3, fracción IX de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.		

DIRECCIÓN DE ÁREA SERVICIOS GENERALES

DATOS DE IDENTIFICACIÓN			
	Día	Mes	Año
Fecha de Elaboración	08	03	2019
Sujeto Obligado	Comisión Estatal del Agua de Jalisco		
Unidad Administrativa Responsable	Departamento de Compras Gubernamentales		
CONTENIDO DEL SISTEMA			
Finalidad de sistemas y los usos previstos	Ser parte del padrón interno de proveedores		
Personas o grupos de personas sobre las cuales se obtienen los datos	Proveedores		
Procedimiento de recolección	Física		
Tipo de soporte en donde se contienen los datos personales	ELIMINADO. Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Su publicación pondría en riesgo a la Comisión pues reflejaría las posibles vulnerabilidades de soportes de contenidos de datos personales y sus lugares de resguardo.		
Características del lugar de resguardo			
ESTRUCTURA BÁSICA DEL SISTEMA Y LA DESCRIPCIÓN DE LOS TIPOS DE DATOS INCLUIDOS			
DATOS GENERALES DEL SISTEMA			
Área	Responsable	Cargo	
Dirección de Área Servicios Generales	Hermilio de la Torre Delgadillo	Director de Área Servicios Generales	

<table>
<tr><td colspan="4">ADMINISTRADORES</td></tr>
<tr><td>Área</td><td colspan="2">Administrador</td><td>Cargo</td></tr>
<tr><td>Dirección de Área Servicios Generales</td><td colspan="2">Martha Leticia Marquez Tapia</td><td>Jefe del Departamento de Compras Gubernamentales</td></tr>
<tr><td>Dirección de Área Servicios Generales</td><td colspan="2">Martha Gabriela Guerra Luna</td><td>Auxiliar de Compras</td></tr>
<tr><td colspan="4">DATOS PERSONALES INCLUIDOS EN EL SISTEMA/INVENTARIO</td></tr>
<tr><td colspan="4">TIPO DE DATOS PERSONALES</td></tr>
<tr><td colspan="4">Nombre, RFC, Domicilio, teléfono, correo electrónico, información fiscal</td></tr>
<tr><td>Tipo de Tratamiento</td><td colspan="3">Tratamiento no automatizado y automatizado. El que sea requerido, siempre y cuando sea lícito, conforme a las nuevas medidas de seguridad.</td></tr>
<tr><td colspan="4">TRANSFERENCIA DE LA QUE PUEDE SER OBJETO LA INFORMACIÓN CONFIDENCIAL</td></tr>
<tr><td colspan="2">Los datos obtenidos no son transferibles</td><td colspan="2">Los datos obtenidos no son transferibles</td></tr>
<tr><td rowspan="3">Nivel de protección exigible.</td><td>x</td><td colspan="2">Básico</td></tr>
<tr><td></td><td colspan="2">Medio</td></tr>
<tr><td></td><td colspan="2">Alto</td></tr>
<tr><td colspan="4">FUNDAMENTACIÓN</td></tr>
<tr><td colspan="4">Art. 3, fracción IX de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.</td></tr>
</table>

DIRECCIÓN DE ÁREA SERVICIOS GENERALES

DATOS DE IDENTIFICACIÓN			
	Día	Mes	Año
Fecha de Elaboración	08	03	2019
Sujeto Obligado	Comisión Estatal del Agua de Jalisco		
Unidad Administrativa Responsable	Oficialía de Partes/Recepción		
CONTENIDO DEL SISTEMA			
Finalidad de sistemas y los usos previstos	Registro de oficios de particulares/ Bitácora de particulares que ingresan a la CEA		
Personas o grupos de personas sobre las cuales se obtienen los datos	Particulares que quieren tratar algún asunto con alguna de las áreas que integran la CEA y/o dejar solicitud u oficio.		
Procedimiento de recolección	Física/Bitácora		
Tipo de soporte en donde se contienen los datos personales	ELIMINADO. Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Su publicación pondría en riesgo a la Comisión pues reflejaría las posibles vulnerabilidades de soportes de contenidos de datos personales y sus lugares de resguardo.		
Características del lugar de resguardo			
ESTRUCTURA BÁSICA DEL SISTEMA Y LA DESCRIPCIÓN DE LOS TIPOS DE DATOS INCLUIDOS			
DATOS GENERALES DEL SISTEMA			
Área	Responsable	Cargo	

Dirección de Área Servicios Generales	Hermilio de la Torre Delgadillo	Director de Área Servicios Generales

ADMINISTRADORES		
Área	Administrador	Cargo
Dirección de Área Servicios Generales	Percival Iván Pérez Torres	Fotografía y Video (comisionado a Servicios Generales)
DATOS PERSONALES INCLUIDOS EN EL SISTEMA/INVENTARIO		
TIPO DE DATOS PERSONALES		
Nombre y firma		
Tipo de Tratamiento	Tratamiento no automatizado y automatizado. El que sea requerido, siempre y cuando sea lícito, conforme a las nuevas medidas de seguridad.	
TRANSFERENCIA DE LA QUE PUEDE SER OBJETO LA INFORMACIÓN CONFIDENCIAL		
Los datos obtenidos no son transferibles		Los datos obtenidos no son transferibles
Nivel de protección exigible.	x	Básico
		Medio
		Alto
FUNDAMENTACIÓN		
Art. 3, fracción IX de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.		

De las Funciones y Obligaciones de los Servidores Públicos que tratan los Datos Personales.

Para garantizar la aplicación correcta de este sistema es necesario establecer los deberes de los servidores públicos de la CEA 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 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 Unidad de Transparencia.
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 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 de la CEA, 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.
13) 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, conforme los sistemas de tratamiento vigentes deberá:

1) Conocer, aplicar y sujetarse al Aviso de Privacidad y al Documento de Seguridad de la CEA, 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 sistema.
5) Tratar los datos personales para la finalidad para la cual estos fueron recabados según 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 Unidad de Transparencia.

11) Informar a la Unidad de Transparencia sobre los cambios que sufran sus 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 Unidad de Transparencia 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 del la Unidad de Transparencia, 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 de la CEA, 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 Unidad de Transparencia.
6) Aplicar medidas correctivas en caso de identificar incidentes, alteraciones o vulneraciones en el tratamiento de datos personales.
7) Informar a la Unidad de Transparencia sobre los cambios que sufran sus 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 del la Unidad de Transparencia, 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 Unidad de Transparencia.
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 Unidad 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 Unidad de Transparencia y el Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco (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 Unidad 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 de la CEA el aviso de privacidad y el documento de seguridad.
2) Revisión física anual 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 unidades administrativas que tratan datos personales, a través de la Unidad de Transparencia, informes sobre el tratamiento de los datos personales y la aplicación de medidas de seguridad, así como vulneraciones detectadas en el año.

ANÁLISIS DE RIESGOS

Debido a las circunstancias generales, tanto físicas como humanas, en las que se tratan datos personales, se ha 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.

Origen de la Amenaza	**Causa**	**Posibles Consecuencias**
Acceso de personas no autorizadas a los sistemas o plataformas oficiales de la CEA	Adquirir información o datos personales.	Acceso no autorizado. Divulgación de datos personales. Robo de información. Modificaciones no autorizadas.
Personal del sujeto obligado con poco conocimiento sobre el tratamiento de datos personales.	Obtener información para beneficio personal. Curiosidad. Error involuntario. Por fines económicos.	Ataque a otros servidores públicos. Robo de información. Pérdida de datos personales. Uso indebido de datos personales. Uso ilícito de datos personales. Extorsión. Modificaciones no autorizadas.
Daño físico	Corrosión. Agua. Fuego. Accidentes.	Daño o pérdida de los datos personales.
Eventos naturales.	Desastres climatológicos. Fenómenos meteorológicos. 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. Modificaciones no autorizadas.
Decadencias técnicas.	Mantenimiento insuficiente. Falla en equipos. Poca o absoluta renovación de equipos de telecomunicaciones o cómputos. Cambios de voltaje.	Pérdida, destrucción y daño.

Susceptibilidad en redes o sistemas autorizados.	Falta de contraseñas altamente efectivas. Falta de mecanismos para identificar o autenticación de usuarios. Falta de actualización de antivirus.	Pérdida, destrucción y daño. Divulgación y transferencia de datos personales. Modificaciones no autorizadas. Robo de información.
Organización.	Procesos carentes de formalidad para administración, acceso, uso y proceso de archivo.	Pérdida, destrucción y daño. Divulgación y transferencia de datos personales. Modificaciones no autorizadas. Robo de información.
Espacio donde se archiven.	Carencia de un servidor o sistema que almacene los datos personales. La falta de registros, controles o bitácoras, para regular la entrada y salida de personal autorizado al área donde se almacenan o archivan los datos personales (en su caso los expedientes que los contengan), es un escenario de vulneración y riesgo, facilitando el mal manejo de los datos personales y la pérdida, robo o extravío de expedientes.	Daño y/o pérdida de los datos personales. Modificaciones no autorizadas.

Hasta el momento no se han identificado o reportado vulneraciones desde las unidades administrativas generadoras de información que integran la Comisión Estatal del Agua de Jalisco.

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 Unidad de Transparencia con las diferentes Unidades Administrativas de esta CEA.

Las unidades 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 sistema
- El espacio físico o área donde se recaban datos personales, es dentro de las instalaciones o fuera de ellas según las necesidades del área generadora de la información.
- 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.
- Una vez recabados los datos personales, el servidor público genera un expediente, 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 autorizados.

● 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 procedimiento por el cual se obtuvieron los datos personales, los servidores públicos del área tienen acceso a los datos personales.
● Los datos personales recabados se dejan intactos en la carpeta, archivo o expediente del procedimiento al que pertenecen y resguardados por el área responsable de la información.

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.

DE LAS MEDIDAS DE SEGURIDAD

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

Objetivo del 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.
Control de servidores públicos que recaban los datos personales.	Forzosa asistencia a por lo menos a 1 capacitación en materia de datos personales impartida por la Unidad de Transparencia.
Control 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.
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 recabar los datos.
Aviso de privacidad.	Si se cuenta con un formato, este deberá contener la mención y debe dar a conocer el aviso de privacidad de la CEA, ya sea simplificado o la liga de internet que remita al ciudadano al aviso de privacidad. Los formatos nuevos que se impriman posteriores a la emisión del presente documento deberán contar con la liga al aviso de privacidad
Aviso de privacidad.	Si el dato personal fue recabado mediante una plataforma electrónica oficial, esta plataforma deberá contener la mención y debe dar a conocer el aviso de privacidad de la CEA, ya sea simplificado o la liga de internet que remita al ciudadano al aviso de privacidad.
Espacio físico.	ELIMINADO. Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Su publicación pondría en riesgo a la Comisión pues reflejaría las posibles vulnerabilidades de soportes de contenidos de datos personales y sus lugares de resguardo.
Espacio físico.	

Espacio físico.	ELIMINADO. Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Su publicación pondría en riesgo a la Comisión pues reflejaría las posibles vulnerabilidades de soportes de contenidos de datos personales y sus lugares de resguardo.
Espacio físico.	
Archivo	Al finalizar el desahogo de los expedientes estos deberán archivarse en un lugar adecuado con las siguientes características: ELIMINADO. Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Su publicación pondría en riesgo a la Comisión pues reflejaría las posibles vulnerabilidades de soportes de contenidos de datos personales y sus lugares de resguardo.
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: ELIMINADO. Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Su publicación pondría en riesgo a la Comisión pues reflejaría las posibles vulnerabilidades de soportes de contenidos de datos personales y sus lugares de resguardo.
Control de Archivos Electrónicos	ELIMINADO. Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Su publicación pondría en riesgo a la Comisión pues reflejaría las posibles vulnerabilidades de soportes de contenidos de datos personales y sus lugares de resguardo.
Control de Archivos Electrónicos	ELIMINADO. Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Su publicación pondría en riesgo a la Comisión pues reflejaría las posibles vulnerabilidades de soportes de contenidos de datos personales y sus lugares de resguardo.
Inventarios Documentales sobre archivos entregados al CIT	ELIMINADO. Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Su publicación pondría en riesgo a la Comisión pues reflejaría las posibles vulnerabilidades de soportes de contenidos de datos personales y sus lugares de resguardo.
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.

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, misma que deberá seguirse bajo el siguiente formato y ejemplo:

Fecha en la que ocurrió	Motivo	Las acciones correctivas implementadas de forma inmediata y definitiva
05/03/2019	Incendio	Impresión del expediente. Generar nuevo expediente electrónico.

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 el Titular del Órgano Interno de Control.

Medidas de seguridad o controles para la identificación y autentificación de 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:	PÁRRAFO ELIMINADO. Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Controles de identificación y autenticación. Su publicación pondría en riesgo al Instituto pues reflejaría las posibles vulnerabilidades.
Contraseña:	PÁRRAFO ELIMINADO. Información Reservada Artículo 17.1 fracción I inciso a) LTAIPEJM. Controles de identificación y autenticación. Su publicación pondría en riesgo al Instituto pues reflejaría las posibles vulnerabilidades.

Medidas de Seguridad para la Supresión y Borrado Seguro de Datos Personales

Todos los datos personales en posesión del sujeto obligado sin importar el soporte en el que se encuentren deberán ser tratados para la supresión y borrado conforme a las técnicas de supresión y borrado seguro de datos personales.

Las técnicas de supresión y borrado seguro de datos personales son las siguientes:

Métodos Físicos

1. 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.

2. 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.

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.

Los objetivos específicos para la supresión y borrado de datos personales son los siguientes:

- 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 la CEA.
- Servir como base para el proceso adecuado de supresión y borrado de los expedientes que contengan datos personales.
- Guía para depuración de datos personales.

Este apartado es el conjunto de estructuras para el proceso de supresión y borrado de los expedientes que contengan datos personales en posesión del sujeto obligado; por lo tanto los datos personales deberán estar contenidos en archivos apegados a un orden lógico y cronológico.

Bases para supresión y borrado seguro de archivos:

- Las bajas documentales se realizan mediante la aprobación de la Junta de Gobierno.

- Los documentos físicos cuya baja ha sido procedente, se entregan a un reciclador, y estos serán vigilados por personal de la CEA 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.

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 los datos personales se encuentran 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.

Lo anterior toda vez que en la actualidad existen cambios y grandes avances que van modificando la organización de la información, de igual manera no se está exento de nuevos riesgos a futuro.

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.

PLAN DE TRABAJO

La existencia del documento de seguridad, busca enmarcar los deberes de la CEA 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 la CEA 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, dentro de los 6 meses siguientes a la emisión del presente documento:

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 revisará de manera anual, a partir de la emisión del presente documento de seguridad:

1. Revisar lo concerniente al índice de Datos Personales y mantenerlo actualizado.
2. Actualizar las medidas de Seguridad conforme al Sistema de Protección de Datos Personales hecho para la CEA
3. Actualizar el presente plan de trabajo.
4. Se emitirá un programa anual de capacitaciones y además se promoverá que el personal de la CEA se mantenga capacitado no sólo por la Unidad de Transparencia del sujeto obligado, sino también

mediante su asistencia a capacitaciones otorgadas por organismos competentes en la materia.

Mecanismos de Monitoreo y Revisión de 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 la CEA.

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

MECANISMOS DE MONITOREO	OBJETIVO DEL MONITOREO
Visita a 2 (dos) unidades administrativas cada 6 meses. Las unidades de elegirán de manera 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 avances, aplicación, eventualidades y novedades respecto a la aplicación de las medidas de seguridad.

PROGRAMA GENERAL DE CAPACITACIÓN

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

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

CAPACITACIONES

Protección de Datos Personales y Medidas de Seguridad.- En esta capacitación se introducirá a los servidores públicos a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios para poder realizar y administrar correctamente las gestiones y trámites que contienen información confidencial, así como las medidas que deben tomarse para su protección y las implicaciones que existen en caso de no proteger adecuadamente dicha información. Este módulo de capacitación se recomienda para todos los servidores públicos que laboren en la CEA y que manejan datos personales.

Versiones Públicas.- En este módulo se expondrán de manera general los lineamientos que el Sistema Nacional ha desarrollado para la correcta gestión de versiones públicas de documentos que serán entregados o publicados que contengan datos personales y su correcta realización, teniendo como objetivo principal explicar cómo se realiza una versión publica de los documentos que lo requieren y responder dudas sobre el tema que tengan los enlaces de transparencia.

Sistema de Manejo de Protección de Datos Personales.- En este módulo se expondrán de manera general los lineamientos que el Sistema de manejo de datos personales en posesión del sujeto obligado, desarrollado para dar a conocer los nuevos lineamientos con respecto a este sistema, teniendo como objetivo principal explicar cómo se realizan las nuevas actividades que nos permitan desarrollar de forma precisa este sistema.

Solicitudes de Acceso, Rectificación, Cancelación u Oposición de datos personales.- Este módulo está dirigido para el personal de la CEA que maneja datos personales y/o enlaces de transparencia de cada unidad administrativa que da respuesta a las solicitudes de Derechos ARCO, esta capacitación tiene como finalidad instruir a los interesados como deben ser contestadas dichas solicitudes con base a la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Jalisco y sus Municipios. Teniendo como objetivo principal introducir a las bases y generalidades de esta ley, así como resolver dudas de la misma.

Sesión de dudas en Materia del Adecuado Manejo de Datos personales.- En este módulo se expondrán de manera general las posibles actualizaciones del documento de seguridad del sujeto obligado y se atenderán las dudas de los enlaces en materia de transparencia de cada unidad administrativa, para dar seguimiento y cumplimiento a la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Jalisco y sus Municipios.

Bibliografía

- ✓ Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios
  http://congresoweb.congresojal.gob.mx/BibliotecaVirtual/legislacion/Leyes/Ley%20de%20Protecci%C3%B3n%20de%20Datos%20Personales%20en%20Posesi%C3%B3n%20de%20Sujeros%20Obligados.doc

- ✓ Recomendaciones sobre Medidas de Seguridad Aplicables a los Sistemas de Datos Personales
  https://www.gob.mx/cms/uploads/attachment/file/83122/MODELOS_Y_GU_AS_17-pdf

- ✓ GUIA PARA LA ELABORACIÓN DE UN DOCUMENTO DE SEGURIDAD V 1.4
  https://www.ichitaip.org/infoweb/archivos/reader/pdp/Guia_elaboracion_Documento_seguridad.pdf

- ✓ Guía para Elaborar un Documento de Seguridad/formato guía para sujetos obligados. ITEI
  http://www.itei.org.mx/v3/documentos/guias/guia_documento_seguridad_so_31082018.pdf

- ✓ Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.
  http://congresoweb.congresojal.gob.mx/BibliotecaVirtual/legislacion/Leyes/Ley%20de%20Transparencia%20y%20Acceso%20a%20la%20Informaci%C3%B3n%20P%C3%BAblica%20del%20Estado%20de%20Jalisco%20y%20sus%20Municipios.doc

- ✓ Código Civil del Estado de Jalisco
  http://congresoweb.congresojal.gob.mx/BibliotecaVirtual/legislacion/Codigos/C%C3%B3digo%20Civil%20del%20Estado%20de%20Jalisco..doc