

POLÍTICAS INTERNAS PARA LA GESTIÓN Y TRATAMIENTO DE DATOS PERSONALES DEL SISTEMA INTERMUNICIPAL DE LOS SERVICIOS DE AGUA POTABLE Y ALCANTARILLADO SIAPA

OBJETIVO.

Establecer los principios generales que deberán observar los servidores públicos del SIAPA y servirán como guía en el ejercicio de las funciones y proceso de toma de decisiones en materia de protección y tratamiento de los datos personales, en su posesión y resguardo, así como su debida obtención, uso y posterior supresión.

FUNDAMENTO LEGAL.

El artículo 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos, señala que todas las personas tienen derecho a la protección, al acceso, rectificación y cancelación de sus datos personales, así como a manifestar su oposición en los términos que la legislación de la materia lo establezca.

El artículo 4, párrafo sexto, de la Constitución Política del Estado de Jalisco, establece el derecho de toda persona para acceder a la información pública y a la protección de datos personales.

El artículo 30 fracción II de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como su homólogo el artículo 29 punto 1 fracción II de la Ley de protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios; establecen la creación de políticas obligatorias exigibles al interior de la organización del responsable, como un mecanismo que deberá adoptar el responsable para cumplir con el principio de responsabilidad.

El artículo 31 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como su homólogo el artículo 30 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, establecen que los responsables deberán establecer y mantener las medidas de seguridad de carácter físico, técnico y administrativo 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.

El artículo 33 fracción I de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como su homólogo el artículo 32, párrafo 1, fracción I, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, establece la obligación de los responsables a crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión.

El artículo 33 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, se establece el contenido y lo que se deberá incluir en el diseño e implementación de las políticas internas para la gestión y tratamiento de los datos personales.

DISPOSICIONES GENERALES.

I. El tratamiento de datos personales por parte del personal adscrito al SIAPA, deberá sujetarse a las facultades y/o atribuciones que la normatividad aplicable le confiera; y estar justificado por finalidades concretas, lícitas, explícitas y legítimas, en dicho tratamiento se deberán observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad.

II. Previo a recabar datos personales, se deberá mostrar el aviso de privacidad integral, focalizado y/o corto, según corresponda; el aviso de privacidad debe encontrarse publicado en la página web del SIAPA y estar en un lugar visible en todas las áreas administrativas que recaben datos personales.

III. Al momento de recabar datos personales, se deberá hacer del conocimiento del titular la finalidad con la cual se reciben.

IV. Únicamente se deberán tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para el ejercicio de las facultades o atribuciones del SIAPA.

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

VI. Se deberán adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales que se reciban en ejercicio de las facultades otorgadas.

VII. Para el ejercicio de los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) será necesario que el titular o su representante acredite su identidad.

CONTROLES DE IDENTIFICACIÓN DE USUARIOS.

Los equipos de cómputo deberán contar con usuario y contraseña; la contraseña deberá tener entre 8 y 10 caracteres e incluir al menos una letra mayúscula, otra minúscula, un número y un carácter especial, debiendo ser actualizadas, cuando menos, cada 06 seis meses.

Los servidores públicos del SIAPA, deberán portar en un lugar visible su gafete institucional, durante la jornada laboral.

Los usuarios, proveedores o contratistas que ingresen a las instalaciones del Organismo, deberán registrarse en la caseta de vigilancia con una identificación oficial y deberán portar en un lugar visible su etiqueta de visitante; misma que será proporcionada por personal de vigilancia.

SUPRESIÓN Y BORRADO SEGURO DE LOS DATOS PERSONALES.

Para la supresión y borrado seguro de los datos personales, el personal del SIAPA, deberá sujetarse a los métodos y/o técnicas establecidas en el Documento de Seguridad del Sistema Intermunicipal de los Servicios de Agua Potable y Alcantarillado.

Las Unidades Administrativas deberán contar con una trituradora de papel corte cruzado o en su caso llevar a cabo las gestiones necesarias para la adquisición de; mientras que no se adquiera, dicha área deberá solicitar una prestada al área que cuente con una, para la supresión y borrado seguro de los datos personales, de los documentos en su posesión o resguardo.

Queda estrictamente prohibido la reutilización de documentos (hojas de reciclaje) que contengan datos personales.

REVISIÓN DE LAS MEDIDAS DE SEGURIDAD.

Se deberá realizar un monitoreo y evaluación de los sistemas de seguridad, para garantizar la integridad, disponibilidad y confidencialidad de la información, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción

o el uso, acceso o tratamiento no autorizado, con el objeto de que las medidas de seguridad continúen siendo efectivas e idóneas.

Se deberán realizar un acta por parte del área administrativa correspondiente, cuando se confirme una vulneración a los sistemas de tratamiento de datos personales del Organismo.

RESPONSABLE DEL TRATAMIENTO DE LOS DATOS PERSONALES.

Las presentes políticas son de aplicación y observancia obligatoria para todos los servidores públicos adscritos al Sistema Intermunicipal de los Servicios de Agua Potable y Alcantarillado, que se encuentran llevando a cabo su ejercicio público, por lo que son responsables del tratamiento de datos personales, todos los servidores públicos que, posean, resguarden o tengan acceso a datos personales, con la finalidad de garantizar la confidencialidad, integridad y disponibilidad de los datos en posesión de este sujeto obligado responsable.

DERECHOS DE LOS TITULARES DE LOS DATOS PERSONALES.

- I. Garantizar el derecho que tiene toda persona a la protección de sus datos personales en posesión de este sujeto obligado.
- II. Ser informado a través del aviso de privacidad, respecto de la existencia y características principales del tratamiento al que serán sometidos sus datos personales.
- III. Que sean suprimidos sus datos personales cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad.
- IV. En todo momento el titular o su representante podrán solicitar al responsable el acceso, rectificación, cancelación u oposición al tratamiento de los datos personales.

PROGRAMA DE CAPACITACIÓN.

La Unidad de Transparencia deberá implementar un programa anual de capacitación y actualización sobre los principios, obligaciones y demás deberes en materia de protección de datos personales.

El diseño e implementación del programa anual de capacitación y actualización en materia de datos personales debería contemplar los roles y responsabilidades de cada una de las áreas que llevan a cabo un tratamiento a los datos personales.