CMAS
COMISIÓN MUNICIPAL DE AGUA POTABLE Y SANEAMIENTO DE XALAPA

Xalapa
H. Ayuntamiento 2022 - 2025

POLÍTICA INTERNA EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES.

I. PRESENTACIÓN

La presente política interna se elabora con base en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la Ley 316 de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Veracruz de Ignacio de la Llave, así como el Programa Nacional de Protección de Datos Personales (PRONADATOS) y el Programa Veracruzano de Protección de Datos Personales (PROVEDATOS).

En el marco legal nacional e internacional se reconoce como un derecho fundamental la protección de datos personales y la privacidad de las personas, por lo que esta Comisión Municipal de Agua Potable y Saneamiento de Xalapa, y los servidores públicos municipales que la integran tienen la responsabilidad de mantener principios y prácticas adecuadas que garanticen la confidencialidad de los datos personales que utilizan en el cumplimiento de actividades, de tal manera que mediante una cultura de protección y prevención se genere herramientas que atiendan las características de operación especializada y administrativa de este organismo operador.

El documento se compone de un glosario de términos, marco normativo, antecedentes, ámbito de aplicación, disposiciones generales, recomendaciones básicas generales, derechos de los titulares de los datos personales, consentimiento del titular de los datos personales, ejercicio de los derechos ARCO y portabilidad (acceso, rectificación, cancelación y oposición), y sanciones, que en su conjunto marcan la pauta en el tratamiento de datos personales.

II. Glosario de términos

- **Áreas:** Instancias de los sujetos obligados previstas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes, que cuentan o puedan contar, dar tratamiento, y ser responsables o encargadas de los datos personales.
- **CMAS Xalapa:** Comisión Municipal de Agua Potable y Saneamiento de Xalapa, Veracruz.
- **Datos personales:** Cualquier información concerniente a una persona física identificada o identificable expresada en forma numérica, alfabética, alfanumérica, gráfica, fotográfica, acústica o en cualquier otro formato. Se considera que una persona es identificable cuando su identidad puede determinarse directa o indirectamente a través de cualquier información, siempre y cuando esto no requiera plazos, medios o actividades desproporcionadas.
- **Datos personales sensibles:** Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.
- **Derechos ARCOP:** Derechos de acceso, rectificación, cancelación, oposición y de portabilidad de datos personales.
- **Ley 316:** Ley 316 de Protección de Datos Personales en posesión de Sujetos Obligados para el Estado de Veracruz de Ignacio de la Llave.
- **Medidas de seguridad:** Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales en posesión de los sujetos obligados.
- **Responsable:** Cualquier autoridad, dependencia, entidad, órgano y organismo de los poderes Legislativo, Ejecutivo y Judicial, ayuntamientos, órganos, organismos constitucionales autónomos, tribunales

administrativos, fideicomisos y fondos públicos y partidos políticos del Estado, que decide y determina los fines, medios y demás cuestiones relacionadas con determinado tratamiento de datos personales, es decir, aquellos que tengan carácter de sujeto obligado.

- **Tratamiento:** Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

III. MARCO NORMATIVO

- Constitución Política de los Estados Unidos Mexicanos.
- Constitución Política del Estado de Veracruz de Ignacio de la Llave.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Ley 316 de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Veracruz de Ignacio de la Llave.
- Ley 875 de Transparencia y Acceso a la Información Pública para el Estado de Veracruz de Ignacio de la Llave.
- Programa Nacional de Protección de Datos Personales (PRONADATOS).
- Programa Veracruzano de Protección de Datos Personales (PROVEDATOS).
- Disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales.
- Criterios generales para la instrumentación de medidas compensatorias en el sector público del orden federal, estatal y municipal.
- Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales.

III. ANTECEDENTES

A.- Expedición de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y de su homóloga estatal, la Ley 316 de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Veracruz de Ignacio de la Llave.

B.- El Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales aprobó el Programa Nacional de Datos Personales, conocido como PRONADATOS, a su vez el Instituto Veracruzano de Acceso a la Información y Protección de Datos Personales elaboró el Programa Veracruzano de Protección de Datos Personales que de forma análoga, tienen como línea estratégica la de crear y difundir material relacionado con la seguridad de datos personales.

C.- Aunado a lo anterior de manera permanente se está capacitando a las diversas áreas que conforman esta Comisión, reflejo de ello son las versiones públicas que se realizan para atender solicitudes de información, así como para cumplir con las obligaciones de transparencia.

Asimismo, se han brindado asesorías sobre las medidas que se deben tomar para proteger los datos personales.

IV. POLÍTICA INTERNA

La presente Política Interna en Materia de Protección de Datos Personales, se desarrolló tomando en consideración los artículos 46 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Veracruz de Ignacio de la Llave, cumpliendo con las siguientes disposiciones:

I. Los controles para garantizar que se valida la confidencialidad, integridad y disponibilidad de los datos personales;	Lineamientos generales en materia de clasificación y desclasificación de información, así como para la elaboración de versiones públicas. Manuales de Organización y Procedimientos.
II. Las acciones para restaurar la disponibilidad y el acceso a los datos personales de manera oportuna en caso de un incidente físico o técnico;	Generación de respaldos en la nube. Archivos Físicos.
III. Las medidas correctivas en caso de identificar una vulneración o incidente en los tratamientos de datos personales;	Revisiones a las diferentes áreas administrativas.
IV. El proceso para evaluar periódicamente las políticas, procedimientos y planes de seguridad establecidos, a efecto de mantener su eficacia;	
V. Los controles para garantizar que únicamente el personal autorizado podrá tener acceso a los datos personales para los finalidades concretas, lícitas, explícitas y legítimas que originaron su tratamiento; y	Uso de gafete para el personal que realiza el tratamiento de datos personales o que entra a la base de datos de resguardo de los mismos. Uso de contraseñas para acceder a las bases de datos. Uso de roles en los sistemas, para que cada persona solo acceda a lo que le corresponde.
VI. Las medidas preventivas para proteger los datos personales	Llevar acabo un control y monitoreo permanente sobre las

contra su destrucción accidental o ilícita, su pérdida o alteración y el almacenamiento, tratamiento, acceso o transferencias no autorizadas o acciones que contravengan las disposiciones de la presente Ley y demás que resulten aplicables	medidas de seguridad con las que se cuentan para proteger los datos personales.

1. Objetivo general.

Establecer los principios generales o criterios de acción que sirvan de guía en el proceso de toma de decisiones y en la actuación de los servidores públicos, para garantizar que los datos personales tratados en la competencia de CMAS Xalapa mantengan sus atributos de integridad, confidencialidad y disponibilidad.

2. Ámbito de aplicación:

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

3. Disposiciones Generales:

a. El tratamiento de datos personales deberá sujetarse a las facultades o atribuciones que la normatividad aplicable confiere a esta Comisión, y estar justificado por finalidades concretas, lícitas, explícitas y legítimas (principio de licitud y finalidad).
b. Al momento de recabar datos personales, se deberá poner a disposición del titular el aviso de privacidad correspondiente de

forma física, electrónica o en cualquier formato generado por el responsable para hacer de su conocimiento la finalidad con la cual se recaban (principio de información).

c. Únicamente se podrán tratar datos personales para finalidades distintas a las establecidas en el aviso de privacidad, siempre que se cuente con atribuciones y medie el consentimiento del titular de dichos datos (principio de lealtad y consentimiento).
d. No deberá obtenerse ni tratar datos personales, a través de medios engañosos o fraudulentos. (principio de lealtad)
e. Se deberá adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales que se posean en el ejercicio de las facultades otorgadas a la Comisión principio de calidad).
f. Únicamente se deberán tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para el ejercicio de las facultades o atribuciones de la Comisión (principio de proporcionalidad).
g. Para el ejercicio de los derechos ARCOP (Acceso, Rectificación, Cancelación, Oposición y Portabilidad) será necesario que el titular y, en su caso, la identidad y personalidad con la que actúe el representante.
h. Las y los servidores públicos de la Comisión 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 (principio de responsabilidad).

4. Recomendaciones básicas generales.

Como esquema de buenas prácticas, relacionadas al cumplimiento de principios y deberes que rigen el tratamiento de datos personales, el personal de CMAS Xalapa, debe adoptar en el ámbito de funciones operativas y administrativas, las siguientes recomendaciones:

a. Apegarse a lo establecido en los manuales de organización y procedimientos como medida de seguridad administrativa.
b. Portar el gafete del personal de las áreas que realizan tratamiento a datos personales, como medida preventiva de seguridad.
c. Deberán guardar el debido secreto y confidencialidad sobre la información que conozcan en el desarrollo de su trabajo. Esta obligación de guardar secreto subsistirá aún después de finalizar las relaciones laborales con CMAS Xalapa.
d. Está prohibido revelar información institucional, salvo en aquellos casos en que el desempeño de las funciones así lo requieran. No sacar información ni datos personales de las instalaciones salvo en los casos que lo requieran las funciones asignadas, previa autorización, o en los esquemas trabajo en casa que se establezcan en cada área que integra CMAS Xalapa.
e. Cuando se abandone el puesto de trabajo, ya sea temporalmente o al finalizar el horario de trabajo, los equipos de cómputo o mobiliario de resguardo se deben dejar en un estado que impida la visualización de los datos protegidos: bloqueando el equipo con contraseña o desconectándose de las aplicaciones y la red, y apagando el monitor.
f. Con respecto a los equipos portátiles y resto de dispositivos de almacenamiento móviles (teléfonos móviles, memorias USB, etc.), se debe cumplir con:

- Mantenerlos siempre controlados, (no dejar en lugares públicos, taxis, etc.) para evitar su sustracción.
- Reducir y/o eliminar la información que no vaya a ser utilizada.

g. En caso de pérdida o robo de un dispositivo de almacenamiento móvil (portátil, teléfono, memoria USB, etc.) se notificará inmediatamente como incidencia de seguridad al superior jerárquico para que se proceda en los términos que señalen las disposiciones que sean aplicables.

h. Los datos personales que estén bajo su resguardo únicamente deben ser tratados para las finalidades para las que se hayan obtenido, se actualicen de forma periódica y sean cancelados cuando éstos hayan dejado de ser necesarios.

i. En caso de detectar cualquier indicio de problema de seguridad, inmediatamente debe hacerse del conocimiento del superior jerárquico, para que se implementen las acciones correctivas o preventivas que resulten necesarias.

j. No realizar acciones que puedan poner en peligro la seguridad de la información (introducción de software ilegal, envío de información a través de correo electrónico sin las suficientes medidas de seguridad, etc.). Se debe respetar la configuración de aplicaciones corporativas o institucionales (ofimática, antivirus, etc.) de los puestos de trabajo y sólo podrá ser cambiada bajo la autorización del área competente.

k. Considerar que la comunicación o cesión de contraseñas a sistemas o plataformas de información a persona distinta al usuario asignado, es responsabilidad de quien lo realiza, y no lo exime de las consecuencias que su mal uso pudiera originar.

l. Las contraseñas no deberán anotarse o guardarse en lugares visibles o fácilmente accesibles. Cada usuario se responsabiliza de la

confidencialidad de sus contraseñas y, en caso de que sean conocidas fortuita o fraudulentamente por otras personas, debe comunicarlo como incidencia de seguridad al responsable de su administración para proceder a su cambio inmediato.

m. Reducir al máximo el almacenamiento de información confidencial y eliminarla cuando haya dejado de ser necesaria. En caso de crear archivos para uso temporal debe asegurarse su eliminación cuando estos hayan dejado de utilizarse.

n. El correo electrónico institucional no es un gestor documental, los archivos enviados o recibidos deben estar almacenados en los sistemas y carpetas correspondientes, así como seguir un manejo responsable, preventivo hacia los datos personales propios o de terceros.

o. Al utilizar impresoras o fotocopiadoras, debe asegurarse de recoger los originales al finalizar y de que no quedan documentos con datos sensibles en la bandeja de salida. Si las impresoras son compartidas con otros usuarios sin acceso a los datos que están siendo impresos, se deberán retirar los documentos conforme vayan siendo impresos. De forma análoga, al utilizar los escáneres debe asegurarse de recoger los documentos originales.

p. Adoptar medidas cautelares que eviten accesos no autorizados. En los procesos de traslado de soportes o documentos deberán adoptarse medidas dirigidas a impedir el acceso o manipulación por terceros, de manera que, no pueda verse el contenido, sobre todo, si hubieren datos de carácter personal.

q. Mantener debidamente custodiadas las llaves de acceso a oficinas, así como a los archiveros o mobiliario que contenga soportes o documentos en papel con datos de carácter personal.

r. Cerrar con llave la puerta de oficinas, al término de la jornada laboral o cuando deba ausentarse temporalmente de esta ubicación, a fin de evitar accesos no autorizados.

s. Guardar todos los soportes o documentos que contengan información de carácter personal en un lugar seguro, cuando éstos no sean usados, particularmente, fuera de la jornada laboral. Cuando estos soportes o documentos, no se encuentren almacenados, por estar siendo revisados o tramitados, será la persona que se encuentre a su cargo la que deba custodiar e impedir, en todo momento, que un tercero no autorizado pueda tener acceso.

t. Los soportes o documentos en papel deberán ser almacenados siguiendo las reglas aplicables de archivo para la localización y consulta de la información.

u. No tirar soportes o documentos en papel, donde se contengan datos personales, a papeleras o contenedores, de modo que pueda ser legible o fácilmente recuperable la información, o en su defecto, asegurarse que el mecanismo de desecho impida su recuperación total o parcial.

5. Derechos de los titulares de los datos personales.

a. Ser informado a través del aviso de privacidad, respecto de la existencia y características principales del tratamiento al que serán sometidos sus datos personales.

b. Que sean suprimidos sus datos personales cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad.

c. Ser previamente informado, para el caso de que exista alguna transmisión, de quienes serán los destinatarios de sus datos personales.

d. Solicitar la información referente a sus datos personales y ejercitar los derechos ARCOP.

6. Consentimiento del titular de los datos personales:

a. Los datos de carácter personal, sólo podrán ser transmitidos a terceros, previo consentimiento del titular.

b. Los datos personales de carácter sensible, sólo podrán ser objeto de tratamiento si se cuenta con el consentimiento expreso y por escrito del titular. No será necesario el consentimiento del titular en los siguientes casos:

I. Cuando una Ley así lo disponga;

II. Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;

III. Cuando las transferencias que se realicen entre responsables, sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;

IV. Para el reconocimiento o defensa de derechos del titular ante autoridad competente;

V. Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;

VI. Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;

VII. Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico o la presentación de asistencia sanitaria;

VIII. Cuando los datos personales figuren en fuentes de acceso público;

IX. Cuando los datos personales se sometan a un procedimiento previo de asociación; o

X. Cuando el titular de los datos personales sea una persona reportada como desaparecida.

XI. Sean estrictamente necesarios para el ejercicio y cumplimiento de las atribuciones y obligaciones expresamente previstas en las normas que regulan a esta comisión;

XII. Se dé cumplimiento a un mandato legal;

XIII. Se cuente con el consentimiento expreso y por escrito del titular;

XIV. Sean necesarios por razones de seguridad pública, orden público, salud pública o salvaguarda de derechos de terceros.

7. Ejercicio de los derechos ARCOP:

a. En todo momento el titular de los datos personales o su representante legal, podrán solicitar el acceso, rectificación, cancelación, oposición o portabilidad al tratamiento de los datos personales que le conciernen.

b. Para el ejercicio de los derechos ARCOP es necesario que el titular acredite su identidad y, en su caso, la identidad y personalidad con la que actúe el representante.

c. El titular de los datos personales tendrá derecho a acceder a sus datos que obren en posesión de CMAS Xalapa, así como conocer la información relacionada con las condiciones y generalidades de su tratamiento.

d. El titular de los datos personales tendrá derecho a solicitar la rectificación o corrección de sus datos personales, cuando éstos resulten ser inexactos, incompletos o no se encuentren actualizados.

e. El titular de los datos personales tendrá derecho a solicitar la cancelación de sus datos personales de los archivos, registros, expedientes y sistemas, a fin de que ya no estén en posesión de la Comisión y dejen de ser tratados.

f. El titular podrá oponerse al tratamiento de sus datos personales o exigir que se cese en el mismo, cuando se busque evitar un daño o perjuicio al titular o cuando sean objeto de un tratamiento automatizado.

g. El titular podrá solicitar cuando se traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado, el titular tendrá derecho a obtener del responsable una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos.

h. El responsable deberá establecer procedimientos sencillos que permitan el ejercicio de los derechos ARCOP, cuyo plazo de respuesta no deberá exceder de quince días contados a partir del día siguiente a la recepción de la solicitud.

8. Sanciones

De conformidad con el artículo 179 la Ley 316, son causas de sanción por incumplimiento a las obligaciones en la misma y, las siguientes:

I. Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO o de la portabilidad de los datos personales;

II. Incumplir los plazos de atención previstos para responder las solicitudes para el ejercicio de los derechos ARCOP o para hacer efectivo el derecho de que se trate;

III. Ampliar con dolo los plazos previstos en la presente Ley para responder las solicitudes para el ejercicio de los derechos ARCOP de los datos personales;

IV. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;

V. Dar tratamiento a los datos personales en contravención a los principios y deberes establecidos en la Ley 316;

VI. No contar con el aviso de privacidad;

VII. Omitir en el aviso de privacidad alguno de los elementos a que refieren los artículos 30, 31 y 32 de la Ley 316, según sea el caso, y demás disposiciones que resulten aplicables en la materia;

VIII. Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables. La sanción sólo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales;

IX. Incumplir el deber de confidencialidad establecido en el artículo 42 de la Ley 316;

X. No establecer las medidas de seguridad en los términos que establecen los artículos 42, 43, 44 y 45 de la Ley 316;

XI. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad según los artículos 42, 43, 44 y 45 de la Ley 316;

XII. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la Ley 316;

XIII. Obstruir los actos de verificación de la autoridad;

XIV. Crear bases de datos personales en contravención a lo dispuesto en la Ley 316;

XV. No acatar las resoluciones emitidas por el Instituto;

XVI. Aplicar medidas compensatorias en contravención de los criterios que para tales fines establezca el Sistema Nacional;

XVII. Declarar dolosamente la inexistencia de datos personales cuando éstos existan total o parcialmente en los archivos del responsable;

XVIII. No atender las medidas cautelares establecidas por el Instituto;

XIX. Tratar los datos personales de manera que afecte o impida el ejercicio de los derechos fundamentales previstos en la Constitución Política de los Estados Unidos Mexicanos y en la Constitución Política del Estado;

XX. No presentar ante el Instituto la evaluación de impacto a la protección de datos personales en aquellos casos en que resulte obligatoria, de conformidad con lo previsto en la Ley 316 y demás normativa aplicable;

XXI. Realizar actos para intimidar o inhibir a los titulares en el ejercicio de los derechos ARCOP;

XXII. No inscribir los sistemas de datos personales en el registro en el plazo que previene la Ley 316; y

XXIII. Omitir la entrega del informe anual y demás informes que establezcan la normatividad aplicable, o bien, entregar el mismo de manera extemporánea.

Las causas de responsabilidad previstas en las fracciones I, II, V, VIII, XII, XIV, XVII, XIX y XXIII así como la reincidencia en las conductas previstas en el resto de las fracciones, serán consideradas como graves para efectos de su sanción administrativa.

En caso de que la presunta infracción hubiere sido cometida por algún integrante de un partido político, la investigación y, en su caso, sanción, corresponderán a la autoridad electoral competente. Las sanciones **de carácter económico no podrán ser cubiertas con recursos públicos**.

Sin perjuicio de lo anterior, será obligación de todo el personal de cada una de las áreas de esta Comisión el proteger y resguardar debidamente la información que contenga datos personales, para lo cual deberán de tomar las medidas que sean necesarias para evitar que la información o documentos que se encuentran bajo su custodia o de sus personas servidoras públicas o quienes tengan acceso o conocimiento con motivo de su empleo, cargo o comisión, hagan mal uso de esta, la sustraigan, divulguen, alteren o destruyan, sin causa legítima, además de asegurar su custodia, conservación, integridad y disponibilidad.