Documento de Seguridad en Materia de Protección de Datos Personales del Sistema de Agua Potable y Alcantarillado Municipal (SAPAM) de Villa Comaltitlán, Chiapas

(12 de octubre de 2026)

SISTEMA DE AGUA POTABLE Y ALCANTARILLADO MUNICIPAL DE VILLA COMALTITLÁN, CHIAPAS (SAPAM)

DOCUMENTO DE SEGURIDAD EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

Aplicable a la Unidad de Transparencia y a las Coordinaciones Operativa, Comercial, Administrativa y de Cultura del Agua

Control Documental

- **Sujeto obligado:** SAPAM - Sistema de Agua Potable y Alcantarillado Municipal de Villa Comaltitlán, Chiapas.

- **Documento:** Documento de Seguridad en materia de Protección de Datos Personales.

- **Fecha de emisión:** 12 de octubre de 2026.

- **Vigencia:** A partir de su aprobación y hasta su actualización.

- **Responsable de coordinación:** Unidad de Transparencia SAPAM

- **Aprobación:** Comité de Transparencia de SAPAM.

- **Clasificación de trabajo:** Documento de uso institucional y acceso restringido en lo relativo a controles de seguridad.

Índice

1. Presentación
2. Objetivo
3. Alcance
4. Marco jurídico
5. Definiciones
6. Estructura de responsabilidades
7. Inventario de datos personales y sistemas de tratamiento
8. Identificación de tratamientos por área
9. Clasificación y nivel de riesgo
10. Medidas de seguridad administrativas
11. Medidas de seguridad físicas
12. Medidas de seguridad técnicas
13. Análisis de riesgos
14. Análisis de brecha
15. Plan de trabajo
16. Gestión de vulneraciones de seguridad
17. Respaldo, recuperación y continuidad
18. Gestión de terceros y encargados
19. Capacitación y concientización
20. Monitoreo, revisión y actualización
21. Control documental
22. Aprobación
23. Anexos

1. Presentación

El Sistema de Agua Potable y Alcantarillado Municipal de villa Comaltitlán, en cumplimiento de sus responsabilidades institucionales y con el propósito de fortalecer la confianza de la ciudadanía, establece el presente documento en materia de seguridad de la información y protección de datos personales.

La prestación de los servicios de agua potable, alcantarillado y saneamiento implica la generación, recepción, conservación y tratamiento de información de carácter administrativo, técnico, financiero y personal de las personas usuarias, trabajadores, proveedores y demás personal relacionadas con el organismo. En este sentido, resulta indispensable establecer medidas que permitan prevenir, identificar y atender riesgos de seguridad, así como garantizar que los datos personales sean tratados de manera lícita, segura, confidencial y exclusivamente para las finalidades institucionales correspondientes.

El documento busca promover una cultura institucional de protección de la información entre las personas servidoras públicas, estableciendo buenas prácticas para el manejo de expedientes, sistemas informáticos, documentos físicos, bases de datos, contraseñas, equipos de cómputo y demás recursos que contengan información institucional o datos personales. La aplicación de estas disposiciones observará el marco jurídico aplicable en materia de protección de datos personales, archivos, transparencia, seguridad de la información y responsabilidades administrativas.

2. Objetivo

Establecer las medidas administrativas, técnicas y físicas necesarias para garantizar la protección, confidencialidad, integridad y disponibilidad de los datos personales que se recaban, utilizan, almacenan, procesan y transfieren en el ejercicio de las funciones del comité, a fin de prevenir su pérdida, alteración, destrucción, acceso, tratamiento o divulgación no autorizada.

Ejes principales:

- Identificar los tratamientos y sistemas en los que se manejan datos personales.
- Definir funciones y obligaciones de las personas servidoras públicas que intervienen en dichos tratamientos.
- Implementar medidas administrativas, físicas y técnicas acordes con el riesgo.
- Establecer mecanismos para prevenir, detectar, atender y documentar vulneraciones de seguridad (accesos, usos, modificaciones, pérdidas o divulgaciones no autorizadas).
- Establecer un programa de capacitación y mejora continua.
- Facilitar la atención de los derechos de las personas titulares y la coordinación con la Unidad de Transparencia SAPAM.
- Proteger la información de usuarios, trabajadores, proveedores y demás personas relacionadas con el Comité.

3. Alcance

Aplicable a todas las personas servidoras públicas, personal eventual, prestadores de servicios y terceros que, por sus funciones o mediante un encargo autorizado, intervengan en el tratamiento de datos personales bajo responsabilidad de SAPAM.

4. Marco Jurídico

El documento se formula con base en el marco vigente:

- **Constitución Política de los Estados Unidos Mexicanos:** Artículo 16, en materia de protección de datos personales.
- **Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados:** Vigente con última reforma publicada el 14 de noviembre de 2025.
- **Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas:** Publicada y vigente conforme al Periódico Oficial número 113 de fecha 17 de junio de 2026.
- **Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas** y demás disposiciones estatales aplicables.

- Normatividad archivística aplicable a la conservación, transferencia, baja y disposición documental.
- Reglamentos, lineamientos, políticas internas, manuales de organización y procedimientos de SAPAM.

5. Definiciones

- **Datos personales:** Cualquier información concerniente a una persona física identificada o identificable.
- **Datos personales sensibles:** Aquellos que se refieren a la esfera más íntima de su titular o cuya utilización indebida pueda dar origen a discriminación o conllevar un riesgo grave.
- **Tratamiento:** Cualquier operación realizada sobre datos personales (obtención, registro, organización, conservación, consulta, uso, comunicación, transferencia o supresión).
- **Responsable:** El sujeto obligado que decide sobre el tratamiento de datos personales.
- **Persona encargada:** Persona física o moral ajena a la organización que trata datos personales por cuenta del responsable.
- **Medidas de seguridad:** Acciones, actividades, controles o mecanismos administrativos, técnicos y físicos.
- **Vulneración de seguridad:** Pérdida, destrucción, robo, extravío, copia, uso, acceso, tratamiento, daño, alteración o modificación no autorizada.
- **Sistema de tratamiento:** Conjunto organizado de procedimientos, personas, equipos, aplicaciones, bases de datos y soportes que intervienen en un tratamiento.

6. Estructura de Responsabilidades

- **Dirección / Órgano de Gobierno:** Aprobar y respaldar políticas institucionales; proporcionar recursos; promover cumplimiento.
- **Comité de Transparencia:** Coordinar y supervisar acciones de protección de datos; vigilar el cumplimiento del Documento de Seguridad; establecer programas de capacitación.
- **Unidad de Transparencia:** Coordinar la atención de derechos ARCO y obligaciones; asesorar a las áreas; integrar documentación; coordinar la respuesta ante incidentes.
- **Titulares de las Coordinaciones:** Garantizar que el personal bajo su mando cumpla los controles; designar responsables operativos; reportar cambios e incidentes.
- **Personal usuario de datos:** Tratar únicamente los datos necesarios para sus funciones; mantener confidencialidad; aplicar controles y reportar incidentes.

7. Inventario de Datos Personales y Sistemas de Tratamiento

Cada tratamiento cuenta con nombre, área responsable, finalidad, titular, categorías de datos, medios, soporte, ubicación, accesos, transferencias, plazos de conservación, nivel de riesgo y medidas de seguridad:

- **Comercial (Contratos, Padrón y expediente de usuarios):** Nombre, domicilio, teléfono, correo, datos de contrato/cuenta, historial de pagos y adeudos. Soporte digital y físico. Nivel: *Medio/Alto*.
- **Operativa (Órdenes de trabajo y atención de servicios):** Nombre, domicilio, contacto, ubicación del servicio, fotografías cuando proceda. Soporte físico. Nivel: *Medio*.
- **Administrativa (Facturación, pagos, expedientes de personal):** Identificación, datos de contacto, documentación laboral, bancaria y fiscal. Soporte digital y físico. Nivel: *Medio/Alto*.
- **Cultura del Agua (Participantes y actividades):** Nombre, institución, grado/grupo, contacto e imágenes. Soporte digital y físico. Nivel: *Medio*.
- **Transparencia (Derechos ARCO y solicitudes):** Datos identificativos y contenidos en las solicitudes. Soporte digital y físico. Nivel: *Alto*.

8. Identificación de Tratamientos por Área

- **Unidad de Transparencia:** Recepción y seguimiento de derechos ARCO, integración de expedientes de identidad, elaboración de avisos de privacidad y registro de incidentes.
- **Coordinación Operativa:** Atención de reportes, órdenes de trabajo, inspecciones domiciliarias, fotografías de campo y atención de fugas.
- **Coordinación Comercial:** Altas, modificaciones, bajas, contratos, convenios, adeudos, aclaraciones, restricciones de servicio y multas.
- **Coordinación Administrativa:** Expedientes de personal, nómina, gestión de proveedores, viáticos, comprobación de gastos y control de asistencia.
- **Coordinación Cultura del Agua:** Registro de participantes (incluyendo menores de edad), constancias, datos de contacto, fotografías y videos institucionales, así como enlace con CEAS y CONAGUA.

9. Clasificación y Nivel de Riesgo

- **Bajo:** Pocos titulares, datos de contacto básicos, acceso limitado y consecuencias acotadas (ej. registros generales de actividades públicas).
- **Medio:** Volumen relevante, datos identificativos o múltiples patrimoniales (ej. padrón de usuarios, órdenes de trabajo).
- **Alto:** Afectaciones significativas, expedientes de personal, derechos ARCO o bases con gran volumen de información sensible o crítica.

10. Medidas de Seguridad Administrativas

- Contar con políticas internas de protección de datos y confidencialidad.
- Asignar funciones conforme al principio de necesidad de conocer.
- Mantener inventario actualizado de tratamientos.
- Aplicar avisos de privacidad y evitar recopilar datos innecesarios.
- Establecer procedimientos de alta, cambio y baja de accesos.
- Definir plazos de conservación y destrucción segura.
- Realizar análisis de riesgos y brechas al menos anualmente.

11. Medidas de Seguridad Físicas

- Restringir el acceso a archivos y áreas de resguardo de datos personales.
- Mantener expedientes físicos en archiveros y gavetas cerradas; no dejarlos sobre escritorios innecesariamente.
- Controlar estrictamente el préstamo y devolución de expedientes.
- Proteger equipos portátiles contra extravío y evitar que terceros observen pantallas.
- Contar con mecanismos de prevención contra incendios, humedad e inundaciones.

12. Medidas de Seguridad Técnicas

- Uso de cuentas individuales y contraseñas robustas; prohibido compartir credenciales.
- Autenticación multifactor en sistemas de mayor riesgo y bloqueo automático de sesiones inactivas.
- Mantener actualizados sistemas operativos, aplicaciones, antivirus y soluciones de seguridad.
- Realizar respaldos periódicos y verificar su correcta recuperación.
- Restringir el uso de memorias USB y cifrar o proteger las transmisiones de datos.

13, 14 y 15. Análisis de Riesgos, Análisis de Brecha y Plan de Trabajo.

13. Análisis de riesgo.

Sección Clasificada del Documento de Seguridad Apartado del Análisis de Riesgo. Se testa el apartado número 13, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con 10 dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de

Sección Clasificada del Documento de Seguridad Apartado del Análisis de Riesgo. Se testa el apartado número 13, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con 10 dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas

14. ANÁLISIS DE BRECHA

Sección Clasificada del Documento de Seguridad Apartado del Análisis de Riesgo. Se testa el apartado número 14, que contiene el Análisis de Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales 0 afectar la eficacia de los controles de seguridad, de conformidad con 10 dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas

15. PLAN DE TRABAJO

sección Clasificada del Documento de Seguridad Apartado del Análisis de Riesgo. Se testa el apartado número 15, que contiene el Plan de Trabajo, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales 0 afectar la eficacia de los controles de seguridad, de conformidad con 10 dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas

16. Gestión de Vulneraciones de Seguridad

Ante cualquier vulneración, pérdida o acceso no autorizado, se debe seguir el protocolo de actuación:

1. Detectar y reportar el incidente de inmediato al superior y a la Unidad de Transparencia.
2. Preservar la evidencia disponible sin alterar sistemas.
3. Contener el incidente (retirar accesos, aislar equipos).
4. Identificar titulares, sistemas y áreas afectadas.
5. Evaluar el impacto, documentar en bitácora y aplicar medidas correctivas.
6. Determinar si procede informar a los titulares y a la autoridad competente.
7. Realizar análisis de causa raíz y dar seguimiento hasta su cierre.

17. Respaldo, Recuperación y Continuidad

- Identificar sistemas y archivos críticos definiendo la periodicidad de respaldos.
- Almacenar respaldos en ubicaciones separadas y restringidas.
- Probar periódicamente la recuperación de la información y documentar resultados.
- Contar con planes de continuidad ante fallas de energía, red, software o desastres naturales.

18. Gestión de Terceros y Personas Encargadas

- Formalizar contractualmente las obligaciones de confidencialidad, seguridad y limitación de finalidad con terceros que traten datos por cuenta de SAPAM.
- Limitar el acceso exclusivamente a lo necesario y verificar sus medidas de seguridad.
- Asegurar la devolución o supresión segura de los datos al concluir la relación contractual.

19. Capacitación y Concientización

Programa general de capacitación dirigido a servidoras y servidores públicos:

- **Principios y deberes:** Dirigido a todo el personal (Anual / Constancia).
- **Derechos ARCO:** Dirigido a Transparencia y enlaces (Anual / Constancia).
- **Seguridad de información y contraseñas:** Dirigido a todo el personal (Semestral / Constancia).
- **Prevención y reporte de incidentes:** Dirigido a todo el personal (Anual / Constancia).
- **Manejo seguro de expedientes físicos:** Dirigido a áreas Administrativa, Comercial y Operativa (Anual / Constancia).
- **Uso de imágenes y actividades:** Dirigido a Cultura del Agua (Anual / Constancia).

20. Monitoreo, Revisión y Actualización

- Revisión semestral de controles de acceso a sistemas de datos personales.
- Revisión anual del inventario de tratamientos, análisis de riesgos y brechas.
- Actualización inmediata del Documento de Seguridad ante cambios sustanciales o incidentes relevantes.
- Presentación de resultados y avances ante el Comité de Transparencia.

21. Control Documental

12 de octubre 2026 se emitió oficialmente en la página web del H. Ayuntamiento de villa Comaltitlán el documento de seguridad de SAPAM fue revisado por la directora de transparencia Lic. Ana Sofía Madrid Hernández junto con el comité de SAPAM. aprobó por el director de transparencia Ing. Francisco Spond Gonzalez.

22. Aprobación Institucional

El documento cuenta con las validaciones correspondientes de las instancias administrativas y normativas de SAPAM:

- **Titular de SAPAM:** Ing. Jorge Luis Martínez flores
- **Unidad de Transparencia:** Lic. Ana Sofía Madrid Hernández
- **Coordinación Operativa:** Henry Alexander de León Velázquez
- **Coordinación Comercial:** Eludía Rojas Saturno
- **Coordinación Administrativa:** C. P. José Alfredo López Barrios
- **Comité de Transparencia:** Lic. Ana Sofía Madrid Hernández

23. Anexos

Anexo 1. Fuentes Normativas Oficiales Consultadas

1. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas (texto vigente publicado en el Periódico Oficial con reforma del 17 de junio de 2026).
2. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Cámara de Diputados del H. Congreso de la Unión).
3. Legislación del H. Congreso del Estado de Chiapas en materia de transparencia y archivos.