SAPAM
SISTEMA DE AGUA POTABLE Y ALCANTARILLADO MUNICIPAL

¡CUIDEMOS EL AGUA, ES DE TODOS!

DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE LOS DATOS PERSONALES EN POSESIÓN DEL SISTEMA DE AGUA POTABLE Y ALCANTARILLADO MUNICIPAL (SAPAM) DE SAN CRISTÓBAL DE LAS CASAS, CHIAPAS.

ÍNDICE.

I.	Introducción	Página 3
II.	Objetivos y alcances del documento	Página 5
III.	Sistema de Gestión de Seguridad de los Datos Personales en Posesión del Sistema de Agua Potable y Alcantarillado Municipal de San Crstóbal de Las Casas, Chiapas.	Página 8
IV.	Inventario de Datos y de los Sistemas de Tratamiento de Datos Personales del Sistema de Agua Potable y Alcantarillado Municipal de San Cristóbal de Las Casas, Chiapas.	Página 11
V.	Funciones y Obligaciones de las Personas que Tratan Datos Personales.	Página 15
VI.	Analisis de Riesgo y Brecha.	Página 17
VII.	Gestión de Vulneraciones y Plan de Contingencia.	Página 24
VIII.	Medidas de Seguridad Generales.	Página 27
IX.	Plan de Trabajo.	Página 33
X.	Propuesta de Capacitación en Materia de Datos Personales.	Página 38

I. INTRODUCCIÓN.

El Sistema de Agua Potable y Alcantarillado Municipal (SAPAM), en el ejercicio de sus atribuciones y en cumplimiento de sus funciones como organismo responsable de la prestación de los servicios públicos de agua potable, alcantarillado y demás servicios relacionados, realiza el tratamiento de diversos datos personales de usuarios, trabajadores, proveedores, contratistas y ciudadanos.

En virtud de la importancia de la información que se encuentra bajo su resguardo, el SAPAM reconoce la necesidad de establecer mecanismos adecuados para garantizar la protección de los datos personales y evitar su pérdida, alteración, destrucción, acceso, uso, tratamiento o divulgación no autorizada.

El presente Documento de Seguridad de Datos Personales tiene como finalidad establecer las medidas administrativas, técnicas y físicas que deberán implementarse para proteger los datos personales tratados por el SAPAM, procurando preservar en todo momento su confidencialidad, integridad y disponibilidad. Asimismo, establece los criterios y procedimientos necesarios para identificar y gestionar los riesgos asociados al tratamiento de datos personales, así como para prevenir y atender posibles incidentes de seguridad.

Las medidas contempladas en este documento deberán aplicarse durante todo el ciclo de vida de los datos personales, desde su obtención, registro y almacenamiento, hasta su utilización, conservación y, en su caso, eliminación, considerando las características de los sistemas, procesos, instalaciones y recursos empleados por el organismo.

De igual manera, el presente documento establece responsabilidades para las áreas y servidores públicos que participan en el tratamiento de datos personales, promoviendo una cultura institucional de protección y seguridad de la información. Su aplicación contribuirá a fortalecer el cumplimiento de los principios, deberes y obligaciones establecidos en la normativa aplicable en materia de protección de datos personales.

El SAPAM asume el compromiso de mantener y mejorar continuamente sus medidas de seguridad, realizando revisiones y actualizaciones periódicas de este

documento en función de los cambios en sus procesos, sistemas de información, tecnologías, riesgos identificados y disposiciones jurídicas aplicables, con el propósito de garantizar una protección adecuada de los datos personales que se encuentran bajo su responsabilidad.

II. OBJETIVOS Y ALCANCES DEL DOCUMENTO.

II.I. Objetivos generales.

Establecer los criterios, medidas y procedimientos necesarios para identificar, prevenir, controlar y atender los riesgos que puedan afectar la seguridad, continuidad, calidad y confiabilidad de los servicios de agua potable y alcantarillado del municipio de San Cristóbal de Las Casas, Chiapas, protegiendo la infraestructura, al personal, a los usuarios y al medio ambiente.

II.II. Objetivos específicos.

1. Identificar las instalaciones, equipos, procesos y actividades críticas que integran los sistemas de agua potable y alcantarillado.

2. Detectar y evaluar los riesgos físicos, operativos, ambientales, sanitarios y de seguridad que puedan afectar la prestación de los servicios.

3. Establecer medidas preventivas y de control para reducir la probabilidad de incidentes y sus posibles consecuencias.

4. Definir procedimientos de actuación ante emergencias, fallas operativas, contaminación, interrupciones del suministro, inundaciones, incendios y otros eventos que puedan comprometer el servicio.

5. Proteger las fuentes de abastecimiento, sistemas de captación, conducción, almacenamiento, distribución y tratamiento del agua potable.

6. Fortalecer la seguridad de las instalaciones de alcantarillado, colectores, cárcamos, plantas de tratamiento y demás infraestructura asociada.

7. Establecer responsabilidades y líneas de comunicación para el personal encargado de la operación, mantenimiento y atención de emergencias.

8. Promover la capacitación del personal en materia de seguridad, prevención de riesgos y respuesta ante contingencias.

9. Establecer mecanismos de seguimiento, evaluación y actualización del Documento de Seguridad.

10. Contribuir a garantizar la continuidad y confiabilidad de los servicios de agua potable y alcantarillado para la población del municipio.

II.III. Alcances del documento.

El Documento de Seguridad será aplicable a las instalaciones, infraestructura, equipos, procesos, personal y actividades relacionadas con la prestación de los servicios municipales de agua potable y alcantarillado de San Cristóbal de Las Casas, Chiapas.

Su alcance comprenderá, de manera enunciativa y no limitativa:

1. Fuentes de abastecimiento: pozos, manantiales, galerías filtrantes y demás fuentes utilizadas para el suministro de agua.

2. Captación y conducción: obras de captación, líneas de conducción, estaciones de bombeo y equipos electromecánicos.

3. Potabilización y almacenamiento: sistemas de tratamiento, desinfección, tanques, cisternas y estructuras de almacenamiento.

4. Distribución: redes primarias y secundarias, válvulas, estaciones de regulación y demás componentes del sistema.

5. Alcantarillado sanitario y pluvial: redes, colectores, emisores, pozos de visita, cárcamos y estructuras complementarias.

6. Tratamiento de aguas residuales: plantas de tratamiento y sistemas asociados, cuando formen parte de la infraestructura municipal.

7. Instalaciones administrativas y operativas: oficinas, almacenes, talleres, patios, laboratorios y demás espacios relacionados con la operación del sistema.

8. Personal: trabajadores operativos, técnicos, administrativos, contratistas y terceros que desarrollen actividades dentro de las instalaciones.

9. Emergencias y contingencias: procedimientos para responder ante fallas eléctricas o mecánicas, contaminación del agua, fugas, incendios, inundaciones, fenómenos hidrometeorológicos, actos de vandalismo y otras situaciones que puedan afectar la seguridad o continuidad del servicio.

10. Mantenimiento y operación: medidas de seguridad aplicables a las actividades rutinarias y extraordinarias de inspección, reparación, limpieza, mantenimiento y operación de la infraestructura.

El documento deberá considerar las condiciones particulares de San Cristóbal de Las Casas, incluyendo las características de su infraestructura hidráulica, condiciones topográficas y climáticas, crecimiento urbano, vulnerabilidades de las fuentes de abastecimiento y los riesgos que puedan presentarse durante la operación de los sistemas.

Asimismo, deberá establecer los mecanismos para que el documento sea revisado y actualizado periódicamente, especialmente cuando existan modificaciones en la infraestructura, incorporación de nuevas instalaciones, cambios en los procesos de operación o la ocurrencia de incidentes que permitan identificar nuevos riesgos.

III. SISTEMA DE GESTIÓN DE SEGURIDAD DE LOS DATOS PERSONALES EN POSESIÓN DEL SISTEMA DE AGUA POTABLE Y ALCANTARILLADO MUNICIPAL DE SAN CRSTÓBAL DE LAS CASAS, CHIAPAS.

El Sistema de Agua Potable y Alcantarillado Municipal de San Cristóbal de Las Casas, Chiapas, establece e implementa el Sistema de Gestión de Seguridad de los Datos Personales como un conjunto organizado de políticas, procedimientos, acciones, controles y mecanismos destinados a garantizar la protección de los datos personales que se encuentren bajo su posesión, custodia o tratamiento, con independencia del medio físico o electrónico en el que sean recabados, almacenados, utilizados, consultados, comunicados, transferidos o conservados.

El Sistema de Gestión tiene como finalidad identificar y valorar los riesgos que pudieran comprometer la seguridad de los datos personales, considerando las características, naturaleza, volumen y sensibilidad de la información, así como los medios y procesos empleados para su tratamiento, a efecto de establecer medidas de seguridad administrativas, físicas y técnicas proporcionales a los riesgos identificados. Para tal efecto, se contempla la identificación de los tratamientos y procesos que involucren datos personales, la determinación de las áreas y servidores públicos que intervienen en dichos tratamientos, la identificación de los activos y soportes que contienen o permiten el acceso a la información, el análisis de posibles amenazas y vulnerabilidades, la implementación de controles de acceso y mecanismos de protección, la gestión de respaldos y recuperación de información, la capacitación y concientización del personal, así como la supervisión y evaluación periódica de las medidas adoptadas.

Asimismo, el Sistema establece las bases para la prevención, detección, atención, documentación y seguimiento de incidentes y vulneraciones de seguridad que pudieran afectar los datos personales, así como para la actualización de las medidas de protección cuando se presenten cambios en los procesos, sistemas, tecnologías, estructura organizacional o condiciones de riesgo.

De igual forma, una vez integrados y revisados los inventarios de datos personales correspondientes a las distintas áreas administrativas y operativas del Sistema de Agua Potable y Alcantarillado Municipal de San Cristóbal de Las Casas, Chiapas (SAPAM), se estableció la metodología para la elaboración del análisis de riesgos,

con el propósito de identificar y valorar las circunstancias que pudieran comprometer la seguridad de los datos personales durante su tratamiento. Para tal efecto, y atendiendo a lo previsto en el artículo 27, fracción IV, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, las áreas responsables del tratamiento identificaron y valoraron los datos personales de acuerdo con su naturaleza, categoría y ciclo de vida, así como los activos involucrados en los procesos de obtención, registro, organización, almacenamiento, consulta, utilización, comunicación, transferencia, conservación y, en su caso, supresión de la información. Asimismo, se consideraron las posibles consecuencias que una vulneración de seguridad pudiera ocasionar a los titulares de los datos personales, así como las amenazas, vulnerabilidades y demás factores de riesgo relacionados con los procesos y medios físicos y electrónicos utilizados por el SAPAM, teniendo como amenazas y vulnerabilidades las siguientes:

VULNERABILIDADES	AMENZAS
1. Expedientes físicos sin controles adecuados. 2. Equipos sin mecanismos adecuados de protección. 3. Uso de dispositivos externos sin controles. 4. Áreas de archivo sin controles de acceso. 5. Información almacenada sin clasificación.	1. Acceso no autorizado a expedientes de usuarios o trabajadores. 2. Robo o extravío de equipos de cómputo. 3. Pérdida o destrucción de expedientes físicos. 4. Divulgación accidental de información personal. 5. Uso indebido de información por parte de personal autorizado. 6. Alteración o eliminación no autorizada de registros. 7. Incendios, inundaciones u otros eventos que afecten archivos o equipos. 8. Incumplimiento de procedimientos internos de seguridad.

Con base en los resultados obtenidos del análisis de riesgos, el SAPAM ha identificado y fortalecido las medidas de seguridad administrativas, físicas y técnicas necesarias para proteger los datos personales que se encuentran bajo su responsabilidad. Las medidas administrativas comprenden las políticas, procedimientos, controles, responsabilidades y acciones de gestión orientadas a prevenir y controlar los riesgos relacionados con el tratamiento de los datos personales; las medidas físicas corresponden a los mecanismos destinados a proteger las instalaciones, archivos, equipos, documentos, soportes y demás recursos materiales en los que se encuentran contenidos o mediante los cuales se realiza el tratamiento de los datos; mientras que las medidas técnicas comprenden los controles y mecanismos tecnológicos destinados a proteger los sistemas, equipos, aplicaciones, bases de datos, redes y demás recursos digitales utilizados por el SAPAM.

Derivado de este ejercicio, se identificaron áreas de oportunidad y medidas de seguridad que deberán implementarse, fortalecerse o actualizarse, con la finalidad de reducir y, en la medida de lo posible, mitigar los riesgos identificados. En este sentido, el análisis de brecha constituye una herramienta fundamental para determinar el nivel de cumplimiento de las medidas de seguridad existentes, establecer las acciones necesarias para atender las deficiencias detectadas y fortalecer de manera progresiva la protección de los datos personales tratados por el SAPAM, contribuyendo así a preservar su confidencialidad, integridad y disponibilidad, conforme a las obligaciones aplicables en materia de protección de datos personales.

IV. INVENTARIO DE DATOS Y DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES DEL SISTEMA DE AGUA POTABLE Y ALCANTARILLADO MUNICIPAL DE SAN CRISTÓBAL DE LAS CASAS, CHIAPAS.

El inventario comprende los datos personales contenidos en expedientes, formatos, solicitudes, contratos, registros, sistemas informáticos, bases de datos, archivos físicos y electrónicos y demás documentos generados o recibidos por las unidades administrativas del SAPAM. Entre los principales tratamientos se encuentran aquellos relacionados con el registro y administración de usuarios de los servicios de agua potable y alcantarillado, contratación y actualización de cuentas, facturación y recaudación, atención de solicitudes y reportes ciudadanos, integración de expedientes administrativos, gestión de recursos humanos, proveedores y contratistas, así como aquellos derivados del cumplimiento de obligaciones legales y administrativas. Dependiendo de la naturaleza del tratamiento, podrán ser objeto de procesamiento datos de identificación, contacto, domicilio, información relacionada con la prestación y contratación del servicio, datos laborales, fiscales, patrimoniales o financieros, así como cualquier otro dato personal que resulte necesario y pertinente para el cumplimiento de las funciones del organismo.

Asimismo, el inventario identifica los sistemas, aplicaciones, equipos, archivos y demás activos en los que se realiza el tratamiento de datos personales, considerando tanto los medios físicos como los electrónicos, así como las diferentes etapas del ciclo de vida de la información, desde su obtención y registro hasta su utilización, almacenamiento, consulta, comunicación, transferencia, conservación y, cuando corresponda, supresión o eliminación. Para cada sistema de tratamiento se deberán identificar las áreas responsables, el personal que interviene, las finalidades del tratamiento, los datos personales involucrados, los medios de almacenamiento, las posibles transferencias, los plazos de conservación y las medidas de seguridad aplicables.

En ese sentido se encuentra que siete Órganos Administrativos del SAPAM llevan a cabo el tratamiento de datos personales, las cuales se describen:

1. Órgano Interno de Control.

2. Unidad Jurídica
3. Unidad de Transparencia.
4. Coordinación de Archivo General.
5. Dirección Comercial.
6. Departamento de Recursos Humanos.
7. Departamento de Recursos Materiales.

En este sentido, fue posible identificar que en el ejercicio sus atribuciones, 24 procesos en cuyo cauce se actualiza algún tratamiento de datos personales, por lo que, mediante un ejercicio de sistematización, se pudo colegir que dichas actividades pueden ser categorizadas en los siguientes rubros:

ÓRGANO ADMINISTRATIVO	PROCESO O TRATAMIENTO	FINALIDAD
Órgano Interno de Control	1. Denuncias 2. Investigaciones 3. Auditorías 4. Procedimientos administrativos 5. Declaraciones patrimoniales.	Investigar, fiscalizar y dar seguimiento a posibles responsabilidades administrativas y actos de control interno.
Unidad Jurídica	6. Expedientes jurídicos 7. Elaboración de contratos 8. Elaboración convenios 9. Juicios	Atender asuntos legales, elaborar instrumentos jurídicos y representar legalmente al SAPAM.
Unidad de Transparencia	10. Solicitudes de información 11. Derechos ARCO 12. Recursos de revision 13. Elaboración versiones públicas y protección de	Atender solicitudes de acceso a la información y solicitudes para el ejercicio de los derechos ARCO, así como dar cumplimiento a las obligaciones de transparencia, acceso a la información pública y protección de datos personales.

	datos personales.	
Coordinación de Archivo General	14. Recepción, organización, conservación, consulta, 15. Préstamo y transferencia de expedientes con datos personales.	Organizar, clasificar, conservar, resguardar, administrar y facilitar la consulta de documentos y expedientes institucionales, conforme a las disposiciones aplicables en materia de archivos.
Dirección Comercial	16. Padrón de usuarios 17. Contratación de los servicios de agua y drenaje.	Administrar y actualizar el padrón de usuarios, gestionar la prestación y control de los servicios de agua potable y alcantarillado, así como realizar el registro y seguimiento de pagos, adeudos y demás actividades relacionadas con la gestión comercial.
Departamento de Recursos Humanos	18. Expedientes laborales, 19. Contratación de Personal 20. Pago de nómina.	Administrar la relación laboral del personal, incluyendo los procesos de contratación, integración y actualización de expedientes, nómina, prestaciones, asistencia, movimientos de personal y demás asuntos relacionados con la administración de los recursos humanos.
Departamento de Recursos Materiales	21. Registro de proveedores 22. Adquisiciones, 23. Órdenes de compra, 24. Inventarios	Gestionar los procesos de adquisición y contratación de bienes y servicios, administrar la relación con proveedores, controlar inventarios y bienes, así como llevar a cabo las actividades relacionadas con el patrimonio del SAPAM.

Asimismo, durante el proceso de sistematización se observó que los datos personales cuyo tratamiento se lleva a cabo en los 22 procesos identificados, corresponden a las siguientes 4 categorías:

1. De Identificación:
   Nombre, Domicilio, CURP, Fotografía, Huella Dactilar, Número de Seguridad Social, Firma, Edad, Clave Elector, Estado Civil, RFC, Correo Electrónico, No. de Teléfono Personal, Sexo, Información Académica, Fecha y Lugar de Nacimiento, Grado de Estudios Máximo, Nombre tercero interesado y Domicilio Tercero Interesado.

2. Patrimoniales:
   Cuentas Bancarias, CLABE Interbancaria, Institución Bancaria, plaza y sucursal y Tipo de Cuenta.

3. Sensibles:
   Alergias, Enfermedades Crónicas, Estado Físico, Estado Mental, Tipo de Sangre, Afiliaciones Políticas, Capacidades Diferentes, Historia Clínica, Resultados de Evaluación Psicométrica y de Valores, Postura Religiosa.

4. Laborales:
   Área de Adscripción, Cargo, Correo electrónico institucional, Teléfono Institucional, Domicilio laboral, Nombre del Representante Legal y categoría.

V. FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATAN DATOS PERSONALES.

Las personas servidoras públicas del Sistema de Agua Potable y Alcantarillado Municipal (SAPAM) que, con motivo del ejercicio de sus funciones, tengan acceso o realicen algún tratamiento de datos personales, deberán observar las disposiciones aplicables en materia de protección de datos personales, así como las medidas de seguridad administrativas, técnicas y físicas establecidas en el presente Documento de Seguridad.

Para tal efecto, las personas que intervienen en el tratamiento de datos personales tendrán las siguientes funciones y obligaciones:

ÓRGANO ADMINISTRATIVO	NOMBRE Y CARGO DE LAS PERSONAS SERVIDORAS PÚBLICAS QUE TRATAN LOS DATOS PERSONALES	PROCESO O TRATAMIENTO
Órgano Interno de Control.	**Lic. Gerson Laurent Fiocconi Ricci** / Titular del Órgano Interno de Control. **Lic. Guillermo Alberto Carrion Duque de Estrada** / Titular del Area Investigadora del OIC. **Lic. Jorge Augusto Greene Álcazar** / Titular del Área Substanciadora del OIC.	1. Denuncias 2. Investigaciones 3. Auditorías 4. Procedimientos administrativos 5. Declaraciones patrimoniales.
Unidad Jurídica	**Lic. Laura Gabriela Martínez Tovilla** / Jefa de la Unidad Jurídica.	6. Expedientes jurídicos 7. Elaboración de contratos 8. Elaboración convenios 9. Juicios

Unidad de Transparencia.	**Lic. Lizeth Victoria Montoya Gómez** / Responsible de la Unidad de Transparencia.	10. Solicitudes de información 11. Derechos ARCO 12. Recursos de revision 13. Elaboración versiones públicas y protección de datos personales.
Coordinación de Archivo General.	**Dra. Nallely Rubi Hernández Morales** / Coordinadora General de Archivo.	14. Recepción, organización, conservación, consulta, 15. Préstamo y transferencia de expedientes con datos personales.
Dirección Comercial.	**Lic. Gabriel Martínez Palacios** / Director Comercial.	16. Padrón de usuarios 17. Contratación de los servicios de agua y drenaje.
Departamento de Recursos Humanos.	**Lic. Germán Antonio Aguilar Ramírez** / Jefe de Recursos Humanos. **Lic. Martín López López** / Encargado de Capacitación y Profesionalización. **C.P. Silvia Pérez Aranda** / Encargada de Nómina.	18. Expedientes laborales, 19. Contratación de Personal 20. Pago de nómina.
Departamento de Recursos Materiales.	**Ing. José Gonzalo Urbina Hernádez** / Jefe de Recursos Materiales.	21. Registro de proveedores 22. Adquisiciones, 23. Órdenes de compra, 24. Inventarios

VI. ANÁLISIS DE RIESGOS Y DE BRECHA.

El Sistema de Agua Potable y Alcantarillado Municipal (SAPAM), en cumplimiento de sus obligaciones en materia de protección de datos personales, realiza de manera periódica el análisis de riesgos y de brecha de los tratamientos de datos personales que se efectúan en sus diferentes unidades administrativas.

El análisis tiene como finalidad identificar, evaluar y atender los riesgos que puedan comprometer la confidencialidad, integridad y disponibilidad de los datos personales que se encuentran bajo responsabilidad del SAPAM, considerando las características de los datos tratados, las finalidades del tratamiento, los medios utilizados para su procesamiento, almacenamiento y resguardo, así como las posibles consecuencias que pudieran derivarse de una vulneración.

VI.I Análisis de Riesgos.

El análisis de riesgos comprenderá, de manera enunciativa más no limitativa, los siguientes aspectos:

1. Identificación de los tratamientos de datos personales realizados por las unidades administrativas del SAPAM, incluyendo la Unidad Jurídica, Unidad de Transparencia, Coordinación de Archivo General, Dirección Comercial, Departamento de Recursos Humanos y Departamento de Recursos Materiales.

2. Identificación de los datos personales tratados, considerando su naturaleza, volumen, sensibilidad y las condiciones en las que son obtenidos, utilizados, almacenados, consultados, transmitidos o eliminados.

3. Identificación de amenazas y vulnerabilidades que pudieran afectar los datos personales, tales como acceso no autorizado, pérdida, robo, extravío, alteración, destrucción, divulgación indebida, fallas de sistemas, errores humanos, incidentes físicos o tecnológicos y cualquier otro evento que pueda comprometer la seguridad de la información.

4. Valoración de los riesgos, considerando la probabilidad de que ocurra un

incidente y el posible impacto o daño que pudiera ocasionar a los titulares de los datos personales.

5. Identificación de las medidas de seguridad existentes, tanto administrativas como técnicas y físicas, destinadas a prevenir, detectar, contener y mitigar los riesgos identificados.

6. Determinación de los riesgos residuales, una vez consideradas las medidas de seguridad implementadas por el SAPAM.

7. Establecimiento de acciones de prevención y mitigación, priorizando aquellas que permitan reducir los riesgos identificados a niveles aceptables.

Atento a lo anterior, dentro del SAPAM se podrían presentar los siguientes riesgos:

ÓRGANO ADMINISTRATIVO	PROCESO O TRATAMIENTO	RIESGOS
Órgano Interno de Control.	✓ Denuncias ✓ Investigaciones ✓ Auditorías ✓ Procedimientos administrativos ✓ Declaraciones patrimoniales.	→ Acceso no autorizado a expedientes de denuncias, investigaciones y procedimientos. → Divulgación de datos personales y patrimoniales. → Pérdida, alteración o extravío de expedientes.
Unidad Jurídica	✓ Expedientes jurídicos ✓ Elaboración de contratos ✓ Elaboración convenios ✓ Juicios	→ Acceso no autorizado a expedientes de denuncias, investigaciones y procedimientos. → Divulgación de datos personales y patrimoniales. → Pérdida, alteración o extravío de expedientes.
Unidad de Transparencia.	✓ Solicitudes de información ✓ Derechos	→ Divulgación de datos personales en solicitudes de información o versiones

	ARCO ✓ Recursos de revision ✓ Elaboración versiones públicas y protección de datos personales.	públicas. → Acceso no autorizado a expedientes de derechos ARCO y recursos de revisión. → Error u omisión en la protección o testado de datos personales.
Coordinación de Archivo General.	✓ Recepción, organización, conservación, consulta, ✓ Préstamo y transferencia de expedientes con datos personales.	→ Pérdida, extravío o deterioro de expedientes. → Acceso o préstamo de documentos a personas no autorizadas. → Destrucción o transferencia inadecuada de expedientes.
Dirección Comercial.	✓ Padrón de usuarios ✓ Contratación de los servicios de agua y drenaje.	→ Acceso no autorizado al padrón de usuarios. → Divulgación o modificación indebida de datos de los usuarios. → Pérdida de información relacionada con contratos, pagos y adeudos.
Departamento de Recursos Humanos.	✓ Expedientes laborales, ✓ Contratación de Personal ✓ Pago de nómina.	→ Acceso no autorizado a expedientes laborales y nómina. → Divulgación de información personal, laboral o bancaria. → Pérdida, alteración o eliminación indebida de expedientes.
Departamento de Recursos	✓ Registro de proveedores	→ Acceso no autorizado a información de proveedores.

Materiales.	✓ Adquisiciones, ✓ Órdenes de compra, ✓ Inventarios	→ Divulgación o modificación indebida de datos personales. → Pérdida o extravío de documentación de proveedores y adquisiciones.

VI.II. Análisis de Brecha.

El SAPAM realiza el análisis de brecha con la finalidad de identificar las diferencias entre las medidas de seguridad existentes y aquellas que resultan necesarias para prevenir, reducir y atender los riesgos relacionados con el tratamiento de datos personales.

Con base en los procesos identificados en los órganos administrativos, se determinan las siguientes brechas:

ÓRGANO ADMINISTRATIVO	PROCESO O TRATAMIENTO	BRECHA
Órgano Interno de Control.	✓ Denuncias ✓ Investigaciones ✓ Auditorías ✓ Procedimientos administrativos ✓ Declaraciones patrimoniales.	Falta de controles uniformes para el acceso y resguardo de expedientes de denuncias, investigaciones y declaraciones patrimoniales.
Unidad Jurídica	✓ Expedientes jurídicos ✓ Elaboración de contratos ✓ Elaboración convenios ✓ Juicios	Riesgo de acceso o divulgación no autorizada de expedientes, contratos, convenios y juicios.
Unidad de Transparencia.	✓ Solicitudes de información ✓ Derechos	Posibilidad de divulgar datos personales en solicitudes y versiones públicas.

	ARCO ✓ Recursos de revision ✓ Elaboración versiones públicas y protección de datos personales.	
Coordinación de Archivo General.	✓ Recepción, organización, conservación, consulta, ✓ Préstamo y transferencia de expedientes con datos personales.	Falta de controles homogéneos para préstamo, consulta, transferencia y resguardo de expedientes.
Dirección Comercial.	✓ Padrón de usuarios ✓ Contratación de los servicios de agua y drenaje.	Acceso o modificación no autorizada del padrón de usuarios.
Departamento de Recursos Humanos.	✓ Expedientes laborales, ✓ Contratación de Personal ✓ Pago de nómina.	Acceso o divulgación de información laboral, patrimonial y bancaria.
Departamento de Recursos Materiales.	✓ Registro de proveedores ✓ Adquisiciones, ✓ Órdenes de compra, ✓ Inventarios	Falta de controles uniformes para proteger los datos de proveedores contenidos en expedientes y sistemas.

Aunado a ello, se revisan, entre otros, los siguientes elementos:

1. Políticas y procedimientos internos para el tratamiento y protección de datos personales.

2. Controles de acceso físico y lógico a instalaciones, expedientes, equipos y sistemas.

3. Gestión y protección de usuarios, contraseñas y mecanismos de autenticación.

4. Resguardo de expedientes físicos y archivos que contengan datos personales.

5. Seguridad de equipos de cómputo, sistemas, redes y dispositivos de almacenamiento.

6. Procedimientos para respaldos, recuperación y conservación de información.

7. Control de transferencias y comunicaciones de datos personales.

8. Capacitación y concientización del personal que interviene en el tratamiento de datos personales.

9. Procedimientos para la atención y gestión de incidentes de seguridad.

10. Medidas para la disposición, eliminación o destrucción segura de documentos y soportes que contengan datos personales.

11. Cumplimiento de las obligaciones y principios aplicables en materia de protección de datos personales.

VI.III. Plan de trabajo para la atención de Riesgos y Brechas.

Con base en los resultados obtenidos del análisis de riesgos y de brecha, el SAPAM establecerá un plan de trabajo que permita atender las deficiencias detectadas y

fortalecer progresivamente las medidas de seguridad.

1. El plan deberá considerar, según corresponda:
2. El riesgo o brecha identificada.
3. La medida de seguridad que deberá implementarse o fortalecerse.
4. El área responsable de su atención.
5. Las acciones necesarias para su implementación.
6. El nivel de prioridad.
7. El plazo estimado para su cumplimiento.
8. Los recursos necesarios.
9. Los mecanismos para verificar su implementación y eficacia.

Las medidas de seguridad serán revisadas y, en su caso, actualizadas cuando existan cambios en los tratamientos de datos personales, modificaciones en la estructura organizacional, incorporación de nuevos sistemas o tecnologías, cambios normativos, identificación de nuevas amenazas o vulnerabilidades, o cuando ocurra algún incidente de seguridad que pudiera afectar los datos personales.

VII. GESTIÓN DE VULNERACIONES Y PLAN DE CONTINGENCIA.

El Sistema de Agua Potable y Alcantarillado Municipal (SAPAM) establecerá mecanismos para prevenir, detectar, atender, controlar y dar seguimiento a las vulneraciones de seguridad que pudieran afectar los datos personales tratados por sus unidades administrativas.

VII.I Gestión de Vulneraciones.

Se considerará vulneración de seguridad cualquier incidente que implique, entre otros, la pérdida, destrucción, robo, extravío, alteración, acceso, uso o divulgación no autorizada de datos personales.

Ante la identificación de una vulneración, el SAPAM deberá:

- ✓ Detectar y reportar inmediatamente el incidente al responsable del área y a la unidad competente en materia de protección de datos personales.
- ✓ Contener la vulneración, limitando el acceso o uso de los datos personales afectados.
- ✓ Identificar los datos personales comprometidos, las personas afectadas y los sistemas, expedientes o medios involucrados.
- ✓ Evaluar las posibles consecuencias de la vulneración y determinar el nivel de riesgo para los titulares.
- ✓ Implementar medidas correctivas para evitar que el incidente continúe o vuelva a ocurrir.
- ✓ Documentar el incidente, incluyendo fecha, área involucrada, descripción de los hechos, datos afectados, acciones realizadas y medidas adoptadas.
- ✓ Dar seguimiento hasta la conclusión del incidente y verificar la eficacia de las medidas implementadas.

- ✓ En los casos que corresponda, realizar las notificaciones previstas por la legislación aplicable a las autoridades competentes y a los titulares de los datos personales.

Entre las vulneraciones que deberán considerarse se encuentran:

- → Pérdida o robo de expedientes.
- → Acceso no autorizado a sistemas o archivos.
- → Divulgación accidental o intencional de datos personales.
- → Envío de información a destinatarios incorrectos.
- → Pérdida o robo de equipos de cómputo.
- → Alteración o eliminación no autorizada de información.
- → Fallas de sistemas que ocasionen pérdida o indisponibilidad de datos personales.

VII.II. Plan de Contingencia.

El SAPAM contará con un plan de contingencia orientado a mantener o restablecer, en la medida de lo posible, la disponibilidad, integridad y confidencialidad de los datos personales ante situaciones que puedan interrumpir o afectar su tratamiento.

El plan contemplará las siguientes etapas:

1. Identificación del incidente.
   Determinar el tipo de evento, área afectada, información comprometida y alcance inicial.

2. Contención.
   Aislar equipos, sistemas, expedientes o accesos comprometidos para evitar que el incidente se extienda.

3. Recuperación.
   Restablecer los sistemas, archivos o información mediante respaldos y mecanismos disponibles, verificando previamente su integridad.

4. Continuidad de las operaciones.
   Implementar procedimientos alternos para que las áreas puedan continuar con sus funciones esenciales mientras se restablecen los sistemas o procesos afectados.

5. Evaluación y cierre.
   Analizar las causas del incidente, documentar las acciones realizadas y establecer medidas para evitar su repetición.

VII.III. Responsabilidades.

Los órganos administrativos del SAPAM deberán comunicar inmediatamente cualquier vulneración o incidente de seguridad que detecten y colaborar en las acciones de contención, investigación y recuperación.

El personal que tenga acceso a datos personales deberá:

- ✓ Informar inmediatamente cualquier pérdida, acceso no autorizado o divulgación de información.
- ✓ Proteger los documentos y equipos bajo su responsabilidad.
- ✓ No intentar ocultar, alterar o eliminar evidencia relacionada con un incidente.
- ✓ Atender las instrucciones establecidas para la contención y recuperación.
- ✓ Mantener la confidencialidad de la información involucrada.

La implementación del presente plan deberá considerar los recursos humanos, materiales y tecnológicos disponibles en el SAPAM y deberá revisarse periódicamente para garantizar su actualización y eficacia.

VIII. MEDIDAS DE SEGURIDAD GENERALES.

El Sistema de Agua Potable y Alcantarillado Municipal (SAPAM), en su carácter de responsable del tratamiento de datos personales, establecerá, implementará, mantendrá y revisará las medidas de seguridad administrativas, físicas y técnicas necesarias para proteger los datos personales que se encuentren bajo su responsabilidad.

Las medidas de seguridad tendrán como objetivo prevenir, detectar, contener y, en su caso, corregir los riesgos que puedan afectar los datos personales durante las diferentes etapas de su tratamiento, incluyendo su obtención, registro, organización, almacenamiento, consulta, utilización, comunicación, transferencia, conservación y eliminación.

Las medidas deberán guardar relación con la naturaleza de los datos personales tratados, las finalidades del tratamiento, el volumen de información, los medios utilizados y los riesgos identificados en el análisis correspondiente.

VIII.I. Medidas de Seguridad Administrativas.

Las medidas administrativas estarán orientadas a establecer políticas, procedimientos, responsabilidades y controles que permitan garantizar un tratamiento adecuado de los datos personales.

El SAPAM implementará, entre otras, las siguientes medidas:

- ✓ Asignación de responsabilidades.

Determinar las funciones y responsabilidades de las personas servidoras públicas que intervengan en el tratamiento de datos personales, procurando que cada persona tenga acceso únicamente a la información necesaria para el desempeño de sus funciones.

- ✓ Control de funciones.

Establecer claramente las funciones de cada unidad administrativa respecto de la obtención, uso, conservación, consulta, transferencia y eliminación de datos personales.

- ✓ Confidencialidad.

Establecer obligaciones de confidencialidad para las personas que tengan acceso a datos personales con motivo de su empleo, cargo o comisión.

- ✓ Capacitación.

Implementar acciones periódicas de capacitación y sensibilización para el personal que trate datos personales, particularmente en materia de principios, deberes, medidas de seguridad, confidencialidad y atención de incidentes.

- ✓ Inventario de tratamientos.

Mantener actualizado el inventario de los tratamientos de datos personales realizados por las unidades administrativas del SAPAM.

- ✓ Identificación de riesgos.

Realizar periódicamente análisis de riesgos y de brecha para identificar amenazas, vulnerabilidades y deficiencias en las medidas de seguridad.

- ✓ Políticas y procedimientos.

Establecer procedimientos internos para el tratamiento, resguardo, consulta, transferencia, conservación y eliminación de datos personales.

- ✓ Gestión de incidentes.

Contar con mecanismos para reportar, atender, documentar y dar seguimiento a incidentes o vulneraciones de seguridad.

- ✓ Control de accesos.

Determinar los perfiles y niveles de acceso del personal de acuerdo con las funciones que desempeña.

- ✓ Baja o cambio de funciones.

Retirar o modificar oportunamente los permisos de acceso de las personas que cambien de puesto, funciones o concluyan su relación laboral o administrativa con el SAPAM.

- ✓ Gestión documental.

Establecer controles para la organización, conservación, préstamo, consulta,

transferencia y eliminación de expedientes que contengan datos personales.

- ✓ Revisión periódica.

Revisar periódicamente las políticas y procedimientos para determinar si requieren actualización conforme a los cambios en los procesos, sistemas o tecnologías.

- ✓ Supervisión.

Dar seguimiento al cumplimiento de las medidas de seguridad implementadas por las unidades administrativas responsables de los tratamientos.

VIII.II. Medidas de Seguridad Físicas.

Las medidas físicas estarán destinadas a prevenir el acceso no autorizado, pérdida, robo, daño o destrucción de documentos, equipos y soportes que contengan datos personales.

El SAPAM implementará, según corresponda, las siguientes medidas:

- ✓ Mantener los expedientes físicos que contengan datos personales en áreas destinadas para su resguardo.

- ✓ Restringir el acceso a archivos, oficinas, almacenes y demás espacios donde se encuentren documentos con datos personales.

- ✓ Mantener los expedientes organizados e identificados para evitar su pérdida o extravío.

- ✓ Evitar que documentos que contengan datos personales permanezcan sobre escritorios, áreas de atención al público o lugares donde puedan ser consultados por personas no autorizadas.

- ✓ Implementar controles para el préstamo y devolución de expedientes.

- ✓ Mantener registros o bitácoras de consulta y préstamo de expedientes cuando resulte necesario.

- ✓ Evitar que personas ajenas a las áreas responsables tengan acceso directo

a archivos o documentos que contengan datos personales.

- ✓ Resguardar adecuadamente los equipos de cómputo, dispositivos de almacenamiento y demás soportes que contengan información personal.

- ✓ Evitar dejar equipos o documentos con información personal sin supervisión en lugares de acceso público.

- ✓ Establecer medidas para proteger documentos y equipos contra incendios, inundaciones, humedad, polvo, temperaturas extremas u otros factores ambientales que pudieran ocasionar pérdida o deterioro de información.

- ✓ Implementar procedimientos para la destrucción segura de documentos que hayan cumplido su periodo de conservación.

- ✓ Evitar que documentos desechados que contengan datos personales sean depositados directamente en recipientes de basura sin aplicar previamente un método de destrucción adecuado.

VIII.III. Medidas de Seguridad Técnicas.

Las medidas técnicas estarán orientadas a proteger los datos personales tratados mediante sistemas informáticos, equipos de cómputo, redes, dispositivos electrónicos y medios de almacenamiento.

El SAPAM deberá implementar, de acuerdo con sus capacidades y necesidades, las siguientes medidas:

- ✓ Usuarios y contraseñas.

Asignar cuentas individuales al personal que tenga acceso a sistemas que contengan datos personales.

- ✓ Contraseñas seguras.

Establecer criterios para la creación y administración de contraseñas, evitando compartirlas entre personas servidoras públicas.

- ✓ Perfiles de acceso.

Otorgar permisos de acuerdo con las funciones y responsabilidades de cada usuario.

- ✓ Revocación de accesos.

Cancelar oportunamente las cuentas o permisos de personas que ya no requieran acceso a determinada información.

- ✓ Actualización de sistemas.

Mantener actualizados los sistemas operativos, aplicaciones y herramientas utilizadas para el tratamiento de datos personales.

- ✓ Protección contra software malicioso.

Utilizar herramientas de protección contra virus, malware y otras amenazas informáticas.

- ✓ Respaldos.

Realizar respaldos periódicos de la información que resulte necesaria para garantizar su recuperación ante fallas, pérdida o daño.

- ✓ Protección de respaldos.

Mantener los respaldos en lugares o medios seguros y limitar el acceso a ellos al personal autorizado.

- ✓ Protección de equipos.

Implementar medidas para prevenir el acceso no autorizado a equipos de cómputo, servidores y dispositivos utilizados para tratar datos personales.

- ✓ Dispositivos externos.

Controlar el uso de memorias USB, discos externos y otros dispositivos de almacenamiento que puedan contener datos personales.

- ✓ Correo electrónico.

Verificar los destinatarios antes de enviar información que contenga datos personales y evitar el envío de información a cuentas personales o no autorizadas.

- ✓ Transferencia de información.

Implementar mecanismos que permitan proteger los datos personales durante su transferencia o comunicación cuando exista riesgo de acceso no autorizado.

- ✓ Registros de acceso.

Mantener, cuando técnicamente sea posible, registros o bitácoras que permitan identificar accesos, modificaciones o actividades relevantes realizadas en los sistemas.

- ✓ Bloqueo de equipos.

Configurar mecanismos de bloqueo automático de los equipos cuando permanezcan inactivos durante determinado periodo.

- ✓ Eliminación segura.

Implementar mecanismos adecuados para eliminar información electrónica cuando ya no sea necesaria y cuando legalmente proceda su eliminación.

IX. PLAN DE TRABAJO.

El Sistema de Agua Potable y Alcantarillado Municipal (SAPAM) establecerá un Plan de Trabajo para atender las deficiencias y brechas identificadas en el análisis de riesgos de los tratamientos de datos personales, así como para fortalecer las medidas de seguridad administrativas, físicas y técnicas implementadas en las diferentes unidades administrativas.

El Plan de Trabajo tiene como finalidad establecer las acciones necesarias para prevenir, reducir y controlar los riesgos asociados al tratamiento de datos personales, definiendo las actividades que deberán realizarse, las áreas responsables, la prioridad de atención y los plazos estimados para su cumplimiento.

IX.I. Acciones del Plan de Trabajo

ACCIÓN	ÁREA RESPONSABLE	PRIORIDAD
Actualizar el inventario de tratamientos de datos personales de todas las unidades administrativas.	Unidad de Transparencia y áreas responsables	Alta.
Identificar al personal que tiene acceso a datos personales y establecer los niveles de acceso correspondientes.	Todas las áreas.	Alta.
Revisar y fortalecer el resguardo de expedientes físicos que contengan datos personales.	Todas las áreas / Archivo General.	Alta.
Implementar controles para el préstamo, consulta y devolución de expedientes.	Archivo General y áreas responsables.	Alta.
Revisar los permisos de acceso a sistemas, equipos y archivos electrónicos.	Área responsable de sistemas.	Alta.
Cancelar o modificar los accesos de personas que cambien de funciones o dejen de laborar en el SAPAM.	Recursos Humanos / Área responsable de sistemas.	Alta.
Establecer un programa de	Área responsable de	Alta.

respaldos periódicos de información electrónica.	sistemas.	
8 Fortalecer las medidas de seguridad de los equipos de cómputo y dispositivos de almacenamiento.	Área responsable de sistemas / Recursos Materiales.	Alta.
Establecer controles para el uso de memorias USB y dispositivos externos que contengan datos personales.	Área responsable de sistemas	Media.
Establecer un procedimiento para la eliminación y destrucción segura de documentos con datos personales.	Archivo General / Áreas responsables.	Alta.
Fortalecer los mecanismos de revisión y testado de datos personales en las versiones públicas.	Unidad de Transparencia.	Alta.
Establecer controles específicos para la protección de expedientes laborales, nómina y datos bancarios.	Recursos Humanos.	Alta.
Fortalecer los controles de acceso al padrón de usuarios y sistemas comerciales.	Dirección Comercial / Área responsable de sistemas.	Alta.
Implementar controles para proteger los datos personales de proveedores.	Recursos Materiales.	Media.
Establecer un procedimiento para reportar y atender vulneraciones de seguridad.	Unidad de Transparencia / Todas las áreas.	Alta.
Revisar las medidas de seguridad físicas de archivos, oficinas y áreas de resguardo.	Recursos Materiales / Áreas responsables.	Media.
Realizar periódicamente el análisis de riesgos y de brecha.	Unidad de Transparencia / Áreas responsables.	Alta.

XI.II. Responsables de la Ejecución.

Las unidades administrativas del SAPAM serán responsables de implementar las acciones que correspondan a los tratamientos de datos personales que se encuentren bajo su responsabilidad.

- ✓ La Unidad de Transparencia dará seguimiento, dentro del ámbito de sus atribuciones, a las acciones relacionadas con la protección de datos personales y podrá solicitar a las áreas responsables la información necesaria para verificar el avance del Plan de Trabajo.

- ✓ El Departamento de Recursos Humanos participará en las acciones relacionadas con la capacitación del personal, control de movimientos del personal y obligaciones de confidencialidad.

- ✓ El Departamento de Recursos Materiales participará en las acciones relacionadas con la seguridad física de instalaciones, equipos, mobiliario y dispositivos de almacenamiento.

- ✓ La Coordinación de Archivo General participará en las acciones relacionadas con el resguardo, préstamo, conservación, transferencia y eliminación de expedientes.

- ✓ El área responsable de los sistemas y tecnologías de información, en su caso, participará en la implementación de controles de acceso, respaldos, protección de equipos y sistemas, administración de usuarios y demás medidas técnicas.

Las demás unidades administrativas serán responsables de aplicar las medidas de seguridad correspondientes a los tratamientos de datos personales que realicen.

IX.III. Seguimiento del Plan de Trabajo.

El cumplimiento de las acciones establecidas en el presente Plan deberá ser objeto de seguimiento periódico.

Para acreditar el cumplimiento de las acciones, las áreas responsables podrán generar y conservar evidencia documental, tales como:

- ✓ Listas de asistencia y constancias de capacitación.
- ✓ Inventarios de tratamientos de datos personales.
- ✓ Registros de usuarios y permisos de acceso.
- ✓ Bitácoras de préstamo y consulta de expedientes.
- ✓ Reportes de respaldos de información.
- ✓ Procedimientos y políticas internas.
- ✓ Reportes de incidentes de seguridad.
- ✓ Evidencia de eliminación o destrucción segura de documentos.
- ✓ Informes de revisión de sistemas y equipos.
- ✓ Actas, informes o reportes de cumplimiento.

IX.IV. Evaluación y Actualización.

El Plan de Trabajo será revisado periódicamente para determinar el avance de las acciones y verificar si las medidas implementadas han permitido reducir los riesgos identificados.

Asimismo, podrá ser modificado cuando:

- → Se detecten nuevos riesgos o vulnerabilidades.
- → Se incorporen nuevos tratamientos de datos personales.
- → Se implementen nuevos sistemas o tecnologías.

→ Se modifiquen las funciones de las unidades administrativas.

→ Se presente una vulneración de seguridad.

→ Se identifiquen nuevas brechas de seguridad.

→ Se modifique la normatividad aplicable.

Los resultados del seguimiento y evaluación deberán considerarse para la actualización del análisis de riesgos, análisis de brecha y del presente Documento de Seguridad.

El Plan de Trabajo constituye un instrumento de mejora continua mediante el cual el SAPAM dará seguimiento a las acciones necesarias para fortalecer la seguridad de los datos personales y reducir los riesgos asociados a su tratamiento.

X. PROPUESTA DE CAPACITACIÓN EN MATERIA DE DATOS PERSONALES.

El Sistema de Agua Potable y Alcantarillado Municipal (SAPAM), con el propósito de fortalecer la cultura institucional de protección de datos personales y reducir los riesgos derivados de su tratamiento, implementará un programa de capacitación dirigido a las personas servidoras públicas que, con motivo de sus funciones, tengan acceso, manejen o realicen algún tratamiento de datos personales.

La capacitación tendrá como finalidad proporcionar al personal los conocimientos necesarios para identificar, manejar, proteger y tratar adecuadamente los datos personales, así como para prevenir incidentes y vulneraciones de seguridad.

X.I. Personal al que se dirige.

El programa estará dirigido a las personas servidoras públicas del SAPAM que intervengan en el tratamiento de datos personales, particularmente al personal de:

- ✓ Órgano Interno de Control.
- ✓ Unidad Jurídica.
- ✓ Unidad de Transparencia.
- ✓ Coordinación de Archivo General.
- ✓ Dirección Comercial.
- ✓ Departamento de Recursos Humanos.
- ✓ Departamento de Recursos Materiales.
- ✓ Área responsable de sistemas y tecnologías de información.
- ✓ Demás unidades administrativas que realicen tratamientos de datos personales.

La capacitación deberá priorizar al personal que tenga acceso directo a información de usuarios, trabajadores, proveedores, servidores públicos, denunciantes, particulares y demás titulares de datos personales.

X.II. Temario propuesto.

Módulo 1. Protección de Datos Personales.

1.1 Marco conceptual de la protección de datos personales.
1.2. Principios y deberes aplicables al tratamiento de datos personales.
1.3. Derechos ARCO.
1.4. Obligaciones y responsabilidades de los sujetos obligados.

Módulo 2. Seguridad de los Datos Personales.

2.1. Sistemas de tratamiento de datos personales.
2.2. Inventario de datos personales y bases de datos.
2.3. Identificación de riesgos y vulnerabilidades.
2.4. Medidas de seguridad administrativas, físicas y técnicas.
2.5. Análisis de riesgos y análisis de brecha.
2.6. Gestión de incidentes de seguridad.

Módulo 3. Documento de Seguridad.

3.1. Identificación de los sistemas de tratamiento.
3.2. Funciones y responsabilidades del personal que interviene en el tratamiento.
3.3. Controles y medidas de seguridad implementadas.
3.4. Acciones de monitoreo, supervisión y mejora continua.
3.5. Actualización y revisión del Documento de Seguridad.

Módulo 4. Marco Normativo.

4.1. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados.
4.2. Lineamientos y disposiciones aplicables en materia de protección de datos personales.
4.3. Normatividad interna de SAPAM relacionada con el tratamiento y protección de datos personales.

DOCUMENTO DE SEGURIDAD	
SISTEMA DE DATOS PERSONALES PARA EL SISTEMA DE AGUA POTABLE Y ALCANTARILLADO MUNICIPAL (SAPAM) DE SAN CRISTÓBAL DE LAS CASAS, CHIAPAS.	
Fecha de Elaboración del Documento de Seguridad: 30 de septiembre 2026.	Fecha de Última Actualización del Documento de Seguridad: 30 de septiembre de 2026.
Elaboró: Lic. Lizeth Victoria Montoya Gómez Responsable de la Unidad de Transparencia.	Aprobó: Lic. Carlos Alberto González de León. Director General.