

DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES AÑO 2026



1. PRESENTACIÓN

El Sistema de Agua Potable y Alcantarillado Municipal de Arriaga, Chiapas, en adelante SAPAM, en cumplimiento de las disposiciones aplicables en materia de protección de datos personales, establece el presente Documento de Seguridad como instrumento para identificar, organizar y fortalecer las medidas administrativas, físicas y técnicas destinadas a proteger los datos personales que se encuentran bajo su responsabilidad.

El presente documento tiene como finalidad establecer las medidas necesarias para garantizar la confidencialidad, integridad y disponibilidad de los datos personales tratados por las distintas áreas del organismo, desde su obtención hasta su conservación, bloqueo, supresión o destrucción, según corresponda.

Para su elaboración se consideraron las actividades administrativas, comerciales y operativas del SAPAM, así como los tratamientos relacionados con la contratación y prestación del servicio de agua potable y alcantarillado, el padrón de usuarios, la atención de quejas y reportes, el registro de proveedores, los recursos humanos, las declaraciones de situación patrimonial y las actividades de la Unidad de Transparencia.

El Documento de Seguridad constituye una herramienta de gestión que permitirá identificar los riesgos asociados al tratamiento de datos personales, establecer acciones para atender las áreas de oportunidad y dar seguimiento a la implementación de medidas de protección.

Su cumplimiento será obligatorio para las personas servidoras públicas que, en el ejercicio de sus funciones, tengan acceso o intervengan en el tratamiento de datos personales.

El documento deberá revisarse y actualizarse cuando existan modificaciones en los tratamientos, cambios organizacionales, incorporación de nuevas tecnologías, vulneraciones de seguridad o cualquier otra circunstancia que haga necesaria su actualización.

SISTEMA DE AGUA POTABLE Y ALCANTARILLADO MUNICIPAL ARRIAGA

2. OBJETIVO

Establecer las medidas administrativas, físicas y técnicas que permitan proteger los datos personales tratados por el SAPAM, así como definir las responsabilidades y mecanismos de control necesarios para garantizar su adecuado tratamiento.

De manera específica, el presente documento tiene los siguientes objetivos:

- Identificar los tratamientos de datos personales realizados por el SAPAM.
- Identificar las áreas responsables y las personas que intervienen en dichos tratamientos.
- Establecer las funciones y obligaciones del personal que tiene acceso a datos personales.
- Identificar los riesgos y las áreas de oportunidad en materia de seguridad.
- Establecer medidas para prevenir accesos, pérdidas, alteraciones o divulgaciones no autorizadas.
- Definir acciones para fortalecer las medidas de seguridad existentes.
- Establecer mecanismos para atender y documentar vulneraciones.
- Establecer medidas para el respaldo y recuperación de información.
- Determinar mecanismos de monitoreo, revisión y mejora continua.
- Promover la capacitación del personal en materia de protección de datos personales.

3. RESPONSABILIDADES

El SAPAM, como responsable del tratamiento de los datos personales que recaba y utiliza en el ejercicio de sus atribuciones, deberá implementar y mantener las medidas de seguridad necesarias para protegerlos.

3.1. Dirección

La Dirección, a cargo del C.P. Rolando Martínez Toledo, será responsable de autorizar el presente Documento de Seguridad y proporcionar las condiciones institucionales necesarias para la implementación de las medidas establecidas.

Entre sus responsabilidades se encuentran:

- Autorizar el Documento de Seguridad y sus actualizaciones.
- Impulsar el cumplimiento de las medidas de seguridad.
- Proporcionar, conforme a las posibilidades del organismo, los recursos necesarios para atender las áreas de oportunidad.
- Supervisar que las áreas cumplan las medidas que les correspondan.
- Autorizar, cuando proceda, las acciones relacionadas con la disposición documental, conforme a la normatividad aplicable.

3.2. Unidad de Transparencia

La Unidad de Transparencia será responsable de coordinar y dar seguimiento a las actividades institucionales relacionadas con la protección de datos personales.

Le corresponderá:

- Coordinar la elaboración y actualización del Documento de Seguridad.
- Dar seguimiento al inventario de tratamientos.
- Promover la actualización de los avisos de privacidad.
- Coordinar las actividades de capacitación.
- Dar seguimiento al plan de trabajo.
- Promover la implementación de procedimientos para la atención de vulneraciones.
- Coordinar las revisiones periódicas de las medidas de seguridad.
- Apoyar a las áreas en el cumplimiento de sus obligaciones en materia de protección de datos personales.

3.3. Administración

La Administración, a cargo de la C.P. Ana Karina Castillejos Granados, será responsable de proteger los datos personales que se traten en los procedimientos administrativos y de recursos humanos bajo su competencia.

Entre sus obligaciones se encuentran:

- Resguardar los expedientes laborales.
- Proteger la información relacionada con nómina, prestaciones, datos bancarios y asistencia.
- Limitar el acceso a los documentos bajo su responsabilidad.
- Realizar los respaldos de información correspondientes.
- Informar sobre cualquier incidente que pudiera comprometer la seguridad de los datos personales.
- Colaborar en la implementación de las medidas de seguridad.

3.4. Área Comercial

El Área Comercial será responsable de proteger los datos personales relacionados con la contratación, administración y prestación de los servicios de agua potable y alcantarillado. Deberá:

- Proteger los expedientes de contratación de usuarios.

- Resguardar el padrón digital.
- Proteger los recibos, comprobantes y demás documentos relacionados con los cobros.
- Limitar el acceso a la información comercial.
- Realizar los respaldos correspondientes.
- Mantener bajo resguardo los documentos relacionados con convenios, descuentos, cambios de titular, bajas y demás trámites.
- Informar sobre cualquier vulneración o incidente de seguridad.

3.5. Área Operativa

El Área Operativa deberá utilizar los datos personales que reciba únicamente para realizar las actividades necesarias para la prestación del servicio.

Su personal deberá:

- Utilizar únicamente la información necesaria para realizar las órdenes de trabajo.
- Evitar la divulgación de nombres, domicilios y demás datos personales.
- No reenviar información recibida por medios de mensajería sin autorización.
- Informar sobre cualquier pérdida, extravío o acceso no autorizado.
- Cumplir las instrucciones de seguridad que se establezcan para el uso de teléfonos y medios electrónicos.

3.6. Personal autorizado

Toda persona servidora pública que tenga acceso a datos personales deberá utilizarlos exclusivamente para el cumplimiento de sus funciones, mantener la confidencialidad de la información y aplicar las medidas de seguridad que le correspondan.

El acceso a los datos personales deberá limitarse a las personas que lo requieran para el desempeño de sus funciones.

4. ALCANCE

El presente Documento de Seguridad es aplicable a las áreas del SAPAM que realizan tratamientos de datos personales:

- Dirección.
- Administración.
- Área Comercial.
- Área Operativa.
- Unidad de Transparencia.
- Delegado Municipal del Agua, cuando intervenga en el tratamiento de datos personales.

Comprende los datos personales contenidos en expedientes físicos, formatos impresos, archivos electrónicos, bases de datos, equipos de cómputo, memorias USB, teléfonos y demás soportes utilizados para el cumplimiento de las funciones del organismo.

El documento será de observancia obligatoria para todas las personas servidoras públicas que intervengan en cualquier etapa del tratamiento de datos personales.

5. SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES

El SAPAM establecerá un Sistema de Gestión de Seguridad de Datos Personales integrado por políticas, procedimientos, controles y medidas orientados a proteger la información personal que se encuentra bajo su responsabilidad.

El sistema comprenderá las siguientes actividades:

Identificación: reconocer los tratamientos de datos personales realizados por las áreas del organismo, así como los medios físicos y electrónicos utilizados.

Clasificación: identificar la naturaleza de los datos personales tratados y determinar las medidas de protección que correspondan.

Análisis de riesgos: identificar las amenazas y vulnerabilidades que pudieran comprometer la confidencialidad, integridad o disponibilidad de los datos.

Implementación de medidas: aplicar controles administrativos, físicos y técnicos para prevenir o reducir los riesgos identificados.

Monitoreo y revisión: verificar periódicamente el cumplimiento y la eficacia de las medidas implementadas.

Mejora continua: establecer acciones correctivas y preventivas a partir de los resultados de las revisiones, los incidentes y las modificaciones en los tratamientos.

La Unidad de Transparencia coordinará el seguimiento del sistema, con la colaboración de las áreas responsables de los tratamientos.

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

Las personas servidoras públicas que intervengan en el tratamiento de datos personales deberán cumplir las obligaciones establecidas en la legislación aplicable y en el presente Documento de Seguridad.

En particular, deberán:

- Tratar los datos personales conforme a las finalidades autorizadas.
- Evitar el uso de información para fines distintos de aquellos que justificaron su obtención.
- Mantener la confidencialidad de los datos.
- Evitar la consulta, reproducción o divulgación no autorizada.
- Resguardar los documentos y archivos bajo su responsabilidad.
- Utilizar los equipos y medios electrónicos conforme a las instrucciones institucionales.
- Informar inmediatamente cualquier incidente o vulneración.
- Participar en las actividades de capacitación.
- Colaborar con las revisiones y acciones de mejora.

La Administración tendrá a su cargo los tratamientos relacionados con los recursos humanos; el Área Comercial, los relativos a los usuarios y la prestación del servicio; el Área Operativa, la información necesaria para la ejecución de órdenes de trabajo; y la Unidad de Transparencia, los procedimientos que correspondan a sus atribuciones.

La Contralora Municipal, **María Guadalupe Marroquín Espinosa**, tiene acceso a las declaraciones de situación patrimonial conforme a las funciones que le corresponden.

7. RESGUARDO DE LOS SOPORTES FÍSICOS Y ELECTRÓNICOS

El SAPAM utiliza soportes físicos y electrónicos para el tratamiento de datos personales. Por ello, deberán adoptarse medidas que permitan protegerlos contra pérdida, daño, acceso no autorizado o divulgación indebida.

7.1. Soportes físicos

Los expedientes laborales, documentos de contratación, recibos, formatos y demás documentos que contengan datos personales deberán permanecer bajo resguardo del área responsable.

Las oficinas que contienen documentación cuentan con acceso mediante llave; sin embargo, algunos archiveros no tienen cerradura.

Como medida de fortalecimiento, se deberá procurar la instalación de cerraduras en los

archiveros que contengan información personal y establecer controles para la consulta y devolución de expedientes.

Los documentos no deberán permanecer expuestos al público ni abandonarse en espacios de acceso general.

7.2. Soportes electrónicos

El SAPAM cuenta con dos equipos de cómputo en el Área Comercial y uno en Administración.

Los equipos utilizados para el tratamiento de datos personales cuentan con contraseñas y antivirus. Se informó que las cuentas de usuario son individuales.

En Administración, el archivo de nómina también cuenta con contraseña. El acceso al archivo corresponde al personal autorizado para realizar las actividades administrativas. Se deberá mantener el uso de contraseñas individuales y revisar periódicamente que los accesos correspondan a las funciones del personal.

7.3. Acceso a los documentos y sistemas

El acceso a los datos personales deberá limitarse al personal que los necesite para el cumplimiento de sus funciones.

De acuerdo con la información proporcionada:

- Una persona de Administración tiene acceso al archivo de nómina.
- Dos personas tienen acceso al padrón digital.
- El jefe operativo recibe las órdenes de trabajo que contienen nombre y domicilio.
- La Contralora Municipal tiene acceso a las declaraciones de situación patrimonial.

Los accesos deberán revisarse cuando existan cambios de funciones o bajas de personal.

7.4. Traslado de documentos

Cuando sea necesario trasladar documentos o soportes que contengan datos personales, el personal responsable deberá adoptar medidas para evitar su pérdida, extravío o consulta por personas no autorizadas.

SISTEMA DE AGUA POTABLE Y ALCANTARILLADO MUNICIPAL ARRIAGA

8. BITÁCORAS DE ACCESO, OPERACIÓN Y VULNERACIONES

El SAPAM deberá fortalecer los mecanismos de registro y control de las actividades relacionadas con el tratamiento de datos personales.

Para ello, se implementarán mecanismos de documentación que permitan identificar, cuando corresponda, las consultas, modificaciones, respaldos, transferencias y demás operaciones relevantes.

Asimismo, se deberá implementar una bitácora institucional de vulneraciones de seguridad.

La bitácora deberá contener, como mínimo:

- Fecha y hora del incidente.
- Área involucrada.
- Descripción de la vulneración.
- Datos personales comprometidos.
- Causa o motivo, cuando se conozca.
- Medidas de contención adoptadas.
- Acciones correctivas.
- Responsable del seguimiento.
- Fecha de conclusión.

Actualmente no se tiene conocimiento de vulneraciones previas relacionadas con datos personales. Sin embargo, el SAPAM deberá contar con un procedimiento que permita atender y documentar cualquier incidente que llegue a presentarse.

9. INVENTARIO DE LOS TRATAMIENTOS DE DATOS PERSONALES

El inventario de tratamientos permite identificar los datos personales que son objeto de tratamiento, las áreas responsables, las finalidades y los medios utilizados para su almacenamiento y resguardo.

El SAPAM cuenta con aproximadamente **10,000 usuarios registrados, 20 trabajadores y 7 proveedores.**

A continuación, se describen los principales tratamientos identificados.

9.1. Registro de proveedores

Área responsable: Dirección y Administración.

Titulares: Personas físicas proveedoras y personas que actúan como representantes de personas morales.

Datos personales: Nombre, domicilio, teléfono, correo electrónico, RFC, datos fiscales, firma y documentación relacionada con la identificación y acreditación del proveedor, según corresponda.

Finalidad: Integrar y mantener el registro de proveedores y contar con la información necesaria para los procedimientos administrativos y de contratación.

Medio de obtención: Documentación y datos proporcionados por las personas proveedoras.

Almacenamiento: Expedientes físicos y, cuando corresponda, archivos electrónicos.

Acceso: Personal autorizado de las áreas competentes.

Transferencias: No se reportaron transferencias ordinarias de datos personales a otras instituciones. En caso de requerimiento legal, se analizará su procedencia conforme a la normativa aplicable.

Conservación: Conforme a los instrumentos archivísticos aplicables. El instrumento archivístico del SAPAM se encuentra en elaboración.

9.2. Contratación y prestación del servicio de agua potable y alcantarillado

Área responsable: Área Comercial.

Titulares: Personas solicitantes y usuarias del servicio.

Datos personales: Nombre, domicilio, identificación oficial, documento que acredite propiedad o posesión, número de contrato y demás información necesaria para formalizar el servicio.

Finalidad: Formalizar la contratación, identificar a las personas usuarias y gestionar la prestación del servicio de agua potable y alcantarillado.

Medio de obtención: Atención presencial y documentación proporcionada por las personas solicitantes.

Almacenamiento: Expedientes físicos y registros electrónicos.

Acceso: Personal autorizado del Área Comercial.

Conservación: Conforme al instrumento archivístico que resulte aplicable. Mientras se formaliza, la documentación se conservará temporalmente, evitando su eliminación discrecional.

9.3. Padrón digital de usuarios

Área responsable: Área Comercial.

Titulares: Personas usuarias del servicio.

Número aproximado de titulares: 10,000.

Datos personales: Nombre completo, domicilio, número de contrato, pagos y adeudos.

Finalidad: Administrar la información de las personas usuarias, dar seguimiento a los contratos, registrar pagos y adeudos y apoyar la gestión comercial del servicio.

Medio: Electrónico.

Almacenamiento: Equipo de cómputo del Área Comercial.

Acceso: Dos personas autorizadas.

Actualización: Diaria.

Interrelación: El padrón se relaciona con los procesos de contratación, cobros, adeudos, convenios, descuentos, cambios de titular, constancias y bajas.

Medidas existentes: Contraseña, antivirus y respaldos periódicos.

Conservación: Conforme a las disposiciones administrativas y archivísticas aplicables.

9.4. Cortes, suspensiones y reconexiones

Área responsable: Área Comercial y Área Operativa.

Titulares: Personas usuarias del servicio.

Datos personales: Nombre, domicilio, número de contrato, adeudo o saldo y fotografías del medidor o inmueble cuando sean necesarias para documentar el trabajo.

Finalidad: Gestionar y ejecutar los cortes, suspensiones y reconexiones del servicio.

Medio: Formatos impresos y comunicación electrónica.

Acceso: Personal autorizado del Área Comercial y personal operativo que requiera la información para ejecutar la orden de trabajo.

Comunicación interna: Las órdenes de trabajo pueden enviarse mediante WhatsApp a teléfonos personales del personal operativo. Actualmente no existe una instrucción escrita específica sobre el uso de este medio.

Medida por implementar: Establecer reglas para limitar los datos comunicados, proteger los dispositivos y definir el tratamiento de los mensajes una vez concluido el trabajo. También se promoverá el uso de medios institucionales cuando sea posible.

9.5. Quejas, reportes y denuncias relacionadas con el servicio

Área responsable: Área Comercial.

Áreas que intervienen: Área Operativa, cuando sea necesaria su participación para atender el reporte.

Titulares: Personas usuarias y personas que presentan quejas o reportes.

Número aproximado: 12,000 reportes al año, conforme a la información proporcionada.

Datos personales: Nombre, domicilio, teléfono y datos relacionados con el reporte.

Finalidad: Recibir, atender y dar seguimiento a quejas, reportes y denuncias relacionadas con la prestación del servicio.

Medio de obtención: Atención presencial, telefónica, WhatsApp y escritos.

Almacenamiento: Actualmente no existe un registro formal único de todos los reportes.

Medida por implementar: Establecer un registro físico a cargo del Área Comercial que permita documentar la recepción, atención y conclusión de los reportes.

9.6. Declaraciones de situación patrimonial

Área responsable: Contraloría Municipal, conforme a sus atribuciones.

Titulares: Personas servidoras públicas obligadas a presentar declaraciones.

Persona con acceso identificada: María Guadalupe Marroquín Espinosa, Contralora Municipal.

Datos personales: Información identificativa, laboral, patrimonial, económica y financiera contenida en las declaraciones.

Finalidad: Cumplir las obligaciones legales relacionadas con la presentación y revisión de declaraciones de situación patrimonial.

Acceso: Personal autorizado conforme a las atribuciones legales.

Nivel de protección: Reforzado, considerando la naturaleza patrimonial y financiera de la información.

Conservación: Conforme a las disposiciones aplicables y los instrumentos archivísticos correspondientes.

9.7. Solicitudes de acceso a la información y derechos ARCO

Área responsable: Unidad de Transparencia.

Titulares: Personas solicitantes y personas titulares de datos personales.

Número aproximado: 10 solicitudes de acceso a la información y 5 solicitudes de derechos ARCO al año.

Datos personales: Nombre, domicilio, teléfono, correo electrónico, identificación oficial y datos de representación, cuando corresponda.

Finalidad: Recibir, tramitar y dar respuesta a solicitudes de acceso a la información y al ejercicio de los derechos de acceso, rectificación, cancelación y oposición, así como portabilidad cuando resulte aplicable.

Medio de obtención: Plataforma Nacional de Transparencia, escritos físicos y medios electrónicos.

Acceso: Personal autorizado de la Unidad de Transparencia. Cuando sea necesario, podrán intervenir las áreas competentes para atender las solicitudes.

Conservación: Conforme a los instrumentos archivísticos aplicables.

9.8. Expedientes laborales

Área responsable: Administración y Dirección, conforme a sus funciones.

Titulares: Personas servidoras públicas del SAPAM.

Número aproximado: 20 trabajadores.

Datos personales: Nombre, domicilio, CURP, RFC, identificación oficial, acta de nacimiento, currículum, fotografía, contratos, nombramientos y demás documentos relacionados con la relación laboral.

Finalidad: Integrar y conservar la documentación necesaria para la administración de personal.

Medio: Físico.

Almacenamiento: Expedientes resguardados en la oficina de Dirección.

Acceso: Personal autorizado de Administración y Dirección, conforme a sus funciones.

Conservación: Se reportó un plazo interno de tres años. La aplicación definitiva deberá verificarse con el instrumento archivístico correspondiente.

9.9. Nómina

Área responsable: Administración.

Titulares: Personas servidoras públicas del SAPAM.

Datos personales: Nombre, información laboral, percepciones, deducciones y demás datos necesarios para el cálculo y pago de nómina.

Finalidad: Calcular, administrar y documentar el pago de remuneraciones.

Medio: Archivo electrónico de Excel e impresiones para firma.

Almacenamiento: Equipo de cómputo de Administración y documentos impresos.

Acceso: Una persona de Administración. No se reportó acceso directo del Director al archivo de nómina.

Medidas existentes: Contraseña en el equipo y en el archivo de Excel. Se realizan respaldos aproximadamente cada quince días mediante memoria USB.

Conservación: El plazo queda sujeto al instrumento archivístico, actualmente en elaboración.

9.10. Prestaciones y datos bancarios

Área responsable: Administración.

Titulares: Personas servidoras públicas.

Datos personales: Nombre, datos bancarios e información relacionada con prestaciones, incluyendo aguinaldo.

Finalidad: Gestionar y documentar el pago de prestaciones.

Medio: Documentos impresos y archivos administrativos, según corresponda.

Almacenamiento: Documentación integrada en los expedientes o archivos administrativos.

Acceso: Personal autorizado de Administración.

Conservación: Conforme al instrumento archivístico aplicable.

9.11. Incapacidades y documentación médica

Área responsable: Administración.

Titulares: Personas servidoras públicas.

Datos personales: Identificativos y laborales, así como información relacionada con la salud contenida en certificados de incapacidad.

Datos sensibles: Sí, cuando la documentación contenga información de salud.

Finalidad: Justificar ausencias y realizar los trámites administrativos correspondientes.

Medio: Físico.

Almacenamiento: Expedientes laborales.

Acceso: Personal autorizado de Administración.

Medidas: Acceso restringido y resguardo que impida la consulta por personas no autorizadas.

Conservación: Deberá determinarse conforme a la normativa aplicable y al instrumento archivístico.

9.12. Control de asistencia

Área responsable: Administración.

Titulares: Personas servidoras públicas.

Datos personales: Nombre, registro de asistencia y datos relacionados con la jornada laboral.

Finalidad: Controlar y documentar la asistencia del personal.

Medio: Listas impresas.

Almacenamiento: Documentación física bajo resguardo del área correspondiente.

Acceso: Personal autorizado de Administración y Dirección, conforme a sus funciones.

Conservación: Pendiente de determinar conforme al instrumento archivístico.

9.13. Contratación, bajas y movimientos de personal

Área responsable: Administración.

Titulares: Personas servidoras públicas y personas aspirantes, cuando corresponda.

Datos personales: Identificativos, laborales y documentación necesaria para formalizar la contratación, nombramiento o baja.

Finalidad: Documentar el ingreso, modificación o conclusión de la relación laboral.

Medio: Físico.

Almacenamiento: Expedientes laborales.

Acceso: Personal autorizado de Administración y Dirección.

Conservación: Conforme al instrumento archivístico aplicable.

9.14. Convenios, descuentos, constancias, cambios de titular y bajas de usuarios

Área responsable: Área Comercial.

Titulares: Personas usuarias del servicio.

Datos personales: Nombre, domicilio, número de contrato, recibo anterior, identificación oficial y documentos que acrediten propiedad o los requisitos del trámite.

Finalidad: Atender los trámites relacionados con la cuenta y la prestación del servicio.

Medio: Formatos y documentos impresos, además de los registros que correspondan en el padrón digital.

Almacenamiento: Expedientes físicos y padrón digital.

Acceso: Personal autorizado del Área Comercial y Dirección, según las funciones que correspondan.

Conservación: Sujeta al instrumento archivístico aplicable.

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo y Brecha.

Se testa el apartado número 6, 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 lo 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.

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo y Brecha.

Se testa el apartado número 6, 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 lo 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.

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo y Brecha.

Se testa el apartado número 6, 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 lo 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.

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo y Brecha.

Se testa el apartado número 6, 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 lo 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.

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo y Brecha.

Se testa el apartado número 6, 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 lo 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.

Sección Clasificada del Documento de Seguridad, apartado de Gestión y Plan de Contingencia.

Se testa el apartado número 7, que contiene la Gestión de Vulneraciones y Plan de contingencia, toda vez que contiene información sensible sobre la forma en que el sujeto obligado previene, detecta, contiene, responde y recupera la operación ante incidentes de seguridad, de conformidad con lo 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 desclasificación de la información, así como para la elaboración de versiones públicas

17. CONSERVACIÓN, SUPRESIÓN Y BORRADO SEGURO

Los datos personales deberán conservarse únicamente durante el tiempo necesario para cumplir las finalidades que justificaron su tratamiento y las obligaciones legales correspondientes.

El SAPAM cuenta con un instrumento archivístico en elaboración. Por ello, los plazos que aún no se encuentren formalmente determinados deberán establecerse conforme a dicho instrumento y a la normativa aplicable.

En el caso de los expedientes laborales, se reportó un plazo de conservación de tres años. Su aplicación deberá verificarse con el instrumento archivístico correspondiente. Los recibos de cobro se conservan permanentemente en la práctica, aunque deberá revisarse esta situación para asegurar que el plazo sea congruente con las obligaciones administrativas y archivísticas.

Actualmente no existe un procedimiento escrito para la destrucción de documentos o el borrado de archivos electrónicos, ni se han realizado procesos de destrucción de documentos que contengan datos personales.

Como medida de fortalecimiento, el SAPAM deberá establecer un procedimiento que contemple:

- La identificación de los documentos o archivos que pueden suprimirse.
- La verificación del plazo de conservación.

- La autorización correspondiente.
- El método de destrucción o eliminación.
- La identificación de las personas responsables.
- El registro de la actividad realizada.

Cuando proceda la destrucción física, podrá utilizarse la trituración u otro método que impida la reconstrucción del documento. Para archivos electrónicos, deberán utilizarse métodos de eliminación segura adecuados al soporte y a las características de la información.

No deberá realizarse la eliminación discrecional de documentos mientras no se haya determinado su disposición conforme a la normativa aplicable.

Sección Clasificada del Documento de Seguridad, apartado de Gestión y Plan de Contingencia.

Se testa el apartado número 7, que contiene la Gestión de Vulneraciones y Plan de contingencia, toda vez que contiene información sensible sobre la forma en que el sujeto obligado previene, detecta, contiene, responde y recupera la operación ante incidentes de seguridad, de conformidad con lo 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 desclasificación de la información, así como para la elaboración de versiones públicas

Sección Clasificada del Documento de Seguridad, apartado de Gestión y Plan de Contingencia.

Se testa el apartado número 7, que contiene la Gestión de Vulneraciones y Plan de contingencia, toda vez que contiene información sensible sobre la forma en que el sujeto obligado previene, detecta, contiene, responde y recupera la operación ante incidentes de seguridad, de conformidad con lo 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 desclasificación de la información, así como para la elaboración de versiones públicas

19. MECANISMOS DE MONITOREO, REVISIÓN Y MEJORA CONTINUA

La Unidad de Transparencia coordinará el monitoreo y la revisión de las medidas de seguridad, con la colaboración de las áreas responsables.

Se realizará una revisión integral anual y un seguimiento semestral de las acciones del plan de trabajo.

Las revisiones comprenderán:

- Actualización del Documento de Seguridad.
- Actualización del inventario de tratamientos.
- Vigencia de los avisos de privacidad.
- Cumplimiento de las medidas administrativas.
- Condiciones de resguardo físico.
- Protección de equipos y archivos electrónicos.
- Realización y verificación de respaldos.
- Atención y registro de vulneraciones.
- Cumplimiento del plan de trabajo.
- Capacitación del personal.

También podrán realizarse revisiones extraordinarias cuando se presente una vulneración, se modifique un tratamiento, se incorporen nuevas tecnologías, cambie la estructura del organismo o se reforme la normativa aplicable.

Los resultados de las revisiones deberán documentarse, identificando los hallazgos, las acciones correctivas, las personas responsables y los plazos de atención.

20. PROGRAMA GENERAL DE CAPACITACIÓN

El SAPAM implementará un programa general de capacitación en materia de protección de datos personales, dirigido al personal que intervenga en cualquier etapa del tratamiento.

Como antecedente, se informó que una persona recibió capacitación por parte del órgano garante y que existe evidencia de actividades de capacitación mediante listas de asistencia y fotografías.

El objetivo del programa será fortalecer los conocimientos del personal sobre sus obligaciones y promover una cultura institucional de protección de datos personales.

La meta será capacitar al 100 % del personal que intervenga en tratamientos de datos personales.

La capacitación se realizará anualmente y también cuando existan modificaciones relevantes en los tratamientos o se incorpore personal que tenga acceso a datos personales.

Los temas generales comprenderán:

- Principios y deberes de protección de datos personales.
- Confidencialidad y uso adecuado de la información.
- Medidas administrativas, físicas y técnicas.
- Identificación y reporte de vulneraciones.

- Resguardo de expedientes físicos y electrónicos.
- Uso adecuado de contraseñas y dispositivos.
- Conservación y supresión de datos personales.
- Atención de solicitudes de derechos ARCO.

Además, se podrán impartir temas específicos de acuerdo con las funciones de cada área.

La Unidad de Transparencia coordinará las actividades y conservará la evidencia correspondiente, incluyendo listas de asistencia, fotografías, temarios, materiales y constancias, cuando existan.

21. ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD

El presente Documento de Seguridad deberá actualizarse cuando:

- Se produzcan modificaciones sustanciales en los tratamientos de datos personales.
- Se incorporen nuevas tecnologías.
- Se creen o eliminen tratamientos.
- Se presenten vulneraciones de seguridad.
- El monitoreo y la revisión determinen la necesidad de realizar cambios.
- Se modifique la estructura institucional.
- Se reforme la legislación aplicable.
- Se implementen acciones correctivas que requieran modificar las medidas de seguridad.

La Unidad de Transparencia coordinará las actualizaciones y dará seguimiento a su autorización por la Dirección.

22. VIGENCIA

El presente Documento de Seguridad entrará en vigor a partir de su autorización por la Dirección del Sistema de Agua Potable y Alcantarillado Municipal de Arriaga, Chiapas. Permanecerá vigente hasta que sea sustituido o actualizado conforme a las necesidades del organismo y a las disposiciones legales aplicables.