

Documento de Seguridad

En materia de tratamiento de datos personales en posesión del
Comité de Agua Potable y Alcantarillado del Municipio de Tapachula

(Artículo 35 de la LGPDPPSO y 49 a 50 de la LPDPPSOCHIS)

Fecha de elaboración: 17 de septiembre de 2026

Fecha de última actualización: 30 de septiembre de 2026.

Contenido

1.Introducción	3
2.Glosario de acrónimos, términos y conceptos	5
3.Objetivo del documento de seguridad	12
3.1 Objetivos específicos	12
3.2 Alcance del documento.....	12
4. Sistemas de gestión de seguridad de los datos personales	14
5.Inventario de datos personales y de los sistemas de tratamiento o bases de datos personales	17
6.Funciones y obligaciones de las personas que tratan datos personales.....	25
7.Análisis de riesgos y de brecha	28
8.Gestión de vulneraciones y Plan de Contingencia	38
9.Medidas de Seguridad	43
9.1 Medidas administrativas.....	43
9.2 Medidas físicas.....	46
9.2 Medidas técnicas.....	45
10.Plan de trabajo.....	49
11.Propuesta de capacitación en Materia de Datos Personales	54
12.Actualización del documento de seguridad	56

1. INTRODUCCIÓN

El derecho a la protección de los datos personales constituye un derecho humano reconocido en el marco constitucional mexicano y debe ser garantizado por los sujetos obligados en el ámbito de sus respectivas competencias.

El Comité de Agua Potable y Alcantarillado del Municipio de Tapachula, en ejercicio de sus atribuciones, facultades y funciones, realiza diversos tratamientos de datos personales relacionados con sus personas servidoras públicas, usuarios de los servicios de agua potable y alcantarillado, proveedores, prestadores de servicios, beneficiarios de programas, personas solicitantes, así como otras personas físicas que mantienen alguna relación con el Organismo.

Los tratamientos pueden efectuarse mediante medios físicos, electrónicos, digitales, telefónicos y presenciales, por lo que resulta necesario establecer medidas de seguridad administrativas, físicas y técnicas que permitan garantizar la confidencialidad, integridad y disponibilidad de los datos personales.

La elaboración del presente Documento de Seguridad tiene como finalidad establecer el marco institucional para la identificación, protección, gestión, monitoreo y mejora continua de las medidas implementadas para la protección de los datos personales.

En ese contexto, los artículos 35 de la *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*¹ y 49 a 50 de la *Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas*,² establecen como obligación la elaboración de un documento de seguridad, que se define -según la fracción XIV del artículo 3 de la LGPDPPSO y la fracción XIII del artículo 5 de la LPDPPSOCHIS- como el instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

1 Consultable en: <http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf>

2 Consultable en: https://www.asechiapas.gob.mx/download/leyes/LEY_PROTECCION_DATOS_PERSONALES.pdf

De conformidad con lo dispuesto en el Artículo 29 de Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas,¹ el documento deberá contener, al menos, la siguiente información:

- I. El inventario de datos personales y de los sistemas de tratamiento;
- II. Las funciones y obligaciones de las personas que traten datos personales;
- III. El análisis de riesgos;
- IV. El análisis de brecha;
- V. El plan de trabajo;
- VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y
- VII. El programa general de capacitación.

¹ Consultable en: https://www.asechiapas.gob.mx/download/leyes/LEY_PROTECCION_DATOS_PERSONALES.pdf

2. Glosario de acrónimos, términos y conceptos

Para efectos del presente documentos se entenderá por:

Áreas, unidades administrativas u órganos administrativos: Instancias de los sujetos obligados previstas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes, así como en las estructuras orgánicas u organigramas, que poseen y tratan los datos personales.

Autenticidad: Busca asegurar la validez de la información en tiempo, forma y distribución, así como garantizar el origen de la misma, validando a la persona emisora para evitar suplantación de identidades.

Autentificar: Acción de comprobar que la persona es quien dice ser.

Aviso de Privacidad: Al documento puesto a disposición de la persona titular de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus Datos Personales, con el objeto de informarle los propósitos del tratamiento de los mismos.

Bases de datos: Al conjunto ordenado de Datos Personales referentes a una persona identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Bloqueo: A la identificación y conservación de Datos Personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de estas. Durante dicho periodo, los Datos Personales no podrán ser objeto de tratamiento y, transcurrido este, se procederá a su cancelación en la base de datos que corresponda

Categorías de datos personales: De manera enunciativa, más no limitativa: **Datos de identificación** (nombre, CURP, RFC, nacionalidad, firma, etc.) **Datos de contacto** (domicilio, número telefónico, correo electrónico, etc.) **Datos laborales** (puesto, domicilio oficial, correo institucional, etc.) **Datos patrimoniales** (cuentas bancarias, información crediticia, etc.) **Datos académicos** (formación académica y número de cédula profesional) **Datos sobre salud física y/o mental** (enfermedades o padecimientos) **Datos biométricos** (rostro, huella digital o dactilar, iris, retina, etc.) **Datos sensibles** (origen étnico o racial, religión, preferencia sexual, etc.) **Datos de naturaleza pública** (nombre de personas servidoras públicas)

Clasificación: Acto por el cual se determina fundada y motivadamente que la información que posee el COAPATAP es de carácter reservada o confidencial.

Comité de Transparencia: A la instancia a la que hace referencia el artículo 39 de la LTAIPECH.

Cómputo en la nube: Al modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente.

Consentimiento: A la manifestación de la voluntad libre, específica e informada de la persona titular de los datos mediante la cual se efectúa el tratamiento de los mismos.

Control de acceso: Medida de seguridad que permite el acceso únicamente a quien está autorizado para ello, una vez que se ha cumplido con el procedimiento de identificación y autenticación.

Datos Personales: A cualquier información concerniente a una persona identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

Datos Personales Sensibles: A los datos que se refieran a la esfera más íntima de su titular o cuya utilización indebida pueda dar lugar a discriminación o conlleve un riesgo grave para esta. De manera enunciativa más no limitativa, se consideran sensibles los Datos Personales que puedan revelar aspectos como origen étnico o racial, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

Derechos ARCOP: Derechos de acceso, rectificación, cancelación, oposición y portabilidad de datos personales, todos ellos derechos humanos y fundamentales de rango constitucional.

Disociación: Al procedimiento mediante el cual los Datos Personales no pueden asociarse a la persona titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación de la misma.

Disponibilidad: Característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones, garantizando el acceso a la misma y a los recursos relacionados con ella, cada vez que se requiera.

Documentos o documentos de archivo: Al medio que registra un hecho, acto administrativo, jurídico, fiscal o contable producido, recibido y utilizado en el ejercicio de las facultades, competencias o funciones de los sujetos obligados, con independencia de su soporte documental.

Documento de Seguridad: Al instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los Datos Personales que posee.

Encargado: La persona física o moral, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras, trata datos personales a nombre y por cuenta del responsable.

Expediente: A la unidad documental compuesta por documentos de archivo, ordenados y relacionados por un mismo asunto, actividad o trámite producidos u organizados por los sujetos obligados.

Información: Todo aquel conjunto organizado de datos que generan, obtienen, poseen o administran los sujetos obligados como consecuencia del ejercicio de sus atribuciones, facultades, competencias y funciones, cualquiera que sea su soporte y forma de expresión, los cuales se encuentran contenidos en documentos de archivo que generan, obtienen, adquieren, transforman o conservan por cualquier título.

Integridad: Garantizar la exactitud, totalidad y la confiabilidad de la información y los sistemas o métodos de procesamiento, de manera que éstos no puedan ser modificados sin autorización, ya sea accidental o intencionadamente.

Ley General o LGPDPPSO: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Ley Local o Estatal o LPDPPSOCHIS: Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.

Lineamientos: Lineamientos para la Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.

Medidas de seguridad: Al conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los Datos Personales.

Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información o nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación personal, en materia de protección de datos personales.

Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

- a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
- b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
- c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y
- d) Proveer a los equipos que contienen o almacenan.

Medidas de seguridad técnicas: Al conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los Datos Personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

- a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;
- b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus atribuciones;
- c) Revisar la configuración de seguridad en la adquisición, operación desarrollo y mantenimiento del software y hardware, y
- d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de Datos Personales.

Persona encargada: A la persona física o moral, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate Datos Personales a nombre y por cuenta del responsable.

Plataforma Nacional o PNT: A la Plataforma Nacional de Transparencia a la que hacen referencia la Ley General de Transparencia y Acceso a la Información Pública y la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas.

Principios y deberes:

1. **Calidad:** Los datos personales deben ser ciertos, exactos, completos, pertinentes, correctos y actualizados, en relación con la finalidad para la que fueron recabados.
2. **Confidencialidad:** El responsable deberá establecer controles o mecanismos que permitan que todas las personas que intervengan en cualquier fase del tratamiento de los datos personales guarden confidencialidad respecto de éstos, obligación que subsistirá aún después de que dichas personas finalicen su relación con el responsable. En cualquier caso, se deberá garantizar la secrecía y la no difusión de los datos personales sometidos a tratamiento.

3. **Consentimiento:** Toda manifestación previa, de voluntad libre, específica, informada e inequívoca por la que la persona titular acepta, mediante declaración o acción afirmativa, el tratamiento de sus datos personales.
4. **Finalidad:** El responsable está obligado a determinar las finalidades concretas, lícitas, explícitas y legítimas que motivan cada tratamiento de datos personales que efectúe, las cuales deberán ser acordes con las atribuciones, facultades y funciones que la normatividad aplicable le confiere y también deberán estar previstas en el aviso de privacidad que ponga a disposición de la persona titular de los datos personales.
5. **Información:** El responsable deberá informar a la persona titular de los datos personales sobre la existencia y las características principales del tratamiento al que serán sometidos sus datos personales, a través del aviso de privacidad, a fin de que pueda tomar decisiones informadas al respecto.
6. **Lealtad:** El tratamiento de los datos personales se realizará sin que medie dolo, engaño o medios fraudulentos, En todo momento el responsable debe privilegiar la protección de los intereses de la persona titular de los mismos y la expectativa razonable de privacidad, así como no vulnerar su confianza.
7. **Licitud:** Todo tratamiento de datos personales efectuado por el responsable debe sujetarse a las atribuciones, facultades y funciones que la normativa aplicable le ha conferido. De conformidad con este principio, los datos personales deberán tratarse con apego y cumplimiento a lo dispuesto por la legislación mexicana y el derecho internacional.
8. **Proporcionalidad:** El responsable tratará sólo aquellos datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron y que se encuentren previstas en el aviso de privacidad. El responsable tendrá que realizar esfuerzos razonables para que los datos personales tratados sean los mínimos necesarios y limitar el periodo de tratamiento al mínimo indispensable.
9. **Responsabilidad:** El responsable está obligado a implementar los mecanismos que considere convenientes para acreditar el cumplimiento de los principios rectores, deberes y obligaciones establecidas en la Ley, así como rendir cuentas sobre el tratamiento de datos personales en su posesión a la persona titular de los mismos y a las autoridades competentes.
10. **Seguridad:** El responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

Publicación: La difusión en medios físicos o impresos y electrónicos o digitales de información contenida en documentos de archivo.

Responsable: En el sector público son los "sujetos obligados" de las leyes de transparencia y acceso a la información (cualquier autoridad, dependencia, entidad, organismo u órgano de los poderes Ejecutivo, Legislativo y Judicial, así como los organismos u órganos autónomos, los fideicomisos y fondos públicos y los partidos políticos), excepto los sindicatos y las personas físicas y morales que reciban y ejerzan recursos públicos o que realicen o ejerzan actos de autoridad; mientras que en el sector privado son los llamados "sujetos regulados" (personas físicas y morales de carácter privado), excepto las sociedades de información crediticia en determinados supuestos y las personas físicas que lleven a cabo la recolección y almacenamiento de datos personales para uso exclusivamente personal y sin fines de divulgación o utilización comercial, los cuales deciden y determinan finalidades, medios, medidas de seguridad y demás cuestiones relacionadas con el tratamiento de los datos personales que poseen.

Responsable administrador o administrador responsable: La persona servidora pública titular de un área, designada por la persona servidora pública titular del sujeto obligado, que decide sobre el tratamiento físico o automatizado de los datos personales en posesión del área, así como acerca del contenido y la finalidad de los sistemas de tratamiento o bases de datos personales con las que cuenta el área.

Responsable usuario: La persona servidora pública que está autorizada para tratar datos personales.

Sistema(s) de tratamiento: Todo conjunto organizado de archivos, registros, ficheros, bases o bancos de datos personales en posesión de alguna de las áreas de la SESAEC, cualquiera sea la forma o modalidad de su creación, almacenamiento, organización y acceso. Existen dos tipos de sistemas de tratamiento: Físicos: Conjunto ordenado de datos que para su tratamiento están contenidos en registros manuales, impresos, sonoros, magnéticos, visuales u holográficos. Automatizados: Conjunto ordenado de datos que para su tratamiento han sido o están sujetos a un tratamiento informático y que por ende requieren de una herramienta tecnológica específica para su acceso, recuperación o tratamiento.

Soportes físicos: Los medios de almacenamiento identificables a simple vista, que no requieren de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos; es decir, documentos, oficios, formularios impresos llenados "a mano" o "a máquina", fotografías, placas radiológicas, carpetas y expedientes, entre otros.

Supresión: a baja archivística de los datos personales conforme a la normatividad archivística vigente y aplicable, que resulta en la cancelación, eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable.

Tecnología(s) de la información: Se refiere al hardware y software operado por el sujeto obligado o por una tercera persona que procese información en su nombre, para llevar a cabo una función propia, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u cualquier otro tipo.

Titular: La persona física a quien corresponden los datos personales, a ella pertenecen.

Transferencia: Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, responsable o encargado.

Transmisión de datos personales: La entrega total o parcial de datos personales a cualquier persona distinta de la persona titular de los mismos, mediante el uso de medios físicos o electrónicos tales como la interconexión de equipos de cómputo o bases de datos y acceso a redes de telecomunicación, así como a través de la utilización de cualquier otra tecnología que lo permita.

Transmisor: Responsable que posee los datos personales objeto de la transmisión.

Tratamiento: De manera enunciativa, mas no limitativa, cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, utilización, comunicación, difusión, almacenamiento, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de los mismos, hasta su cancelación, supresión o eliminación.

Unidad de Transparencia: Instancia a la que hacen referencia los artículos 85 de la LGPDPPSO¹ y 115 de la LPDPPSOCHIS,² así como los artículos 45 de la Ley General de Transparencia y Acceso a la Información Pública³ y 67 al 69 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas.⁴

1 Consultable en: <http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf>

2 Consultable en: https://www.asechiapas.gob.mx/download/leyes/LEY_PROTECCION_DATOS_PERSONALES.pdf

3 Consultable en: <https://www.diputados.gob.mx/LeyesBiblio/pdf/LGTAIP.pdf>

4- Consultable en: <https://sesaech.gob.mx/storage/legado/docs/normatividad/marco-juridico-estatal/otras-leyes/20250625-ley-de-transparencia-y-acceso-a-la-informacion-publica-del-estado-de-chiapas.pdf>

3. Objetivo del documento de seguridad

El presente Documento de Seguridad tiene por objeto establecer el marco de trabajo institucional para la protección de los datos personales en posesión del COAPATAP, mediante la identificación de los tratamientos que realizan sus áreas administrativas, la determinación de las funciones y obligaciones del personal involucrado, la identificación y valoración de riesgos, la determinación de medidas de seguridad administrativas, físicas y técnicas, así como el establecimiento de mecanismos de monitoreo, capacitación y mejora continua.

3.1 Objetivos específicos

I. Identificar y documentar los tratamientos de datos personales que se realizan en las diferentes unidades administrativas del COAPATAP, así como los tipos de datos personales tratados, sus finalidades, medios de obtención, soportes, ubicación, personas autorizadas para su acceso y, en su caso, las transferencias o remisiones que se efectúen.

II. Mantener actualizado el inventario de datos personales y de los sistemas de tratamiento o bases de datos personales.

III. Establecer y documentar las funciones, obligaciones y responsabilidades de las personas servidoras públicas que intervienen en el tratamiento de datos personales, delimitando los niveles de acceso y las actividades que correspondan a cada área y persona autorizada.

IV. Implementar y fortalecer medidas de seguridad administrativas, físicas y técnicas destinadas a proteger los datos personales contra daño, pérdida, alteración, destrucción o tratamiento, acceso o uso no autorizado, así como a preservar su confidencialidad, integridad y disponibilidad.

V. Establecer mecanismos para la prevención, identificación, atención y seguimiento de vulneraciones de seguridad que pudieran comprometer datos personales en posesión.

VI. Fortalecer la protección de los derechos de las personas titulares de los datos personales

3.2 Alcance del documento

Lo anterior conforme a lo establecido en la LGPDPPSO¹ y la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas² y los Lineamientos para la Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Chiapas.

El presente Documento de Seguridad es de observancia para el Comité de Agua Potable y Alcantarillado del Municipio de Tapachula (COAPATAP) y comprende a todas las unidades administrativas, personas servidoras públicas y demás personas que, en el ámbito de sus atribuciones o mediante autorización correspondiente, intervengan en cualquier actividad relacionada con el tratamiento de datos personales en posesión de este Organismo Operador.

Su alcance comprende los datos personales tratados en sistemas físicos y automatizados, independientemente del medio, formato o modalidad mediante la cual sean obtenidos, almacenados, utilizados, aprovechados, procesados, consultados, comunicados, transferidos, resguardados o eliminados.

Las áreas que forman parte del COAPATAP y que deberán observar el programa, son las siguientes:

- 1.Coordinación de Informática
- 2.Departamento Jurídico
- 3.Órgano Interno de Control
- 4.Unidad de Transparencia
- 5.Departamento de Recursos Humanos
- 6.Departamento de Recursos Materiales y Servicios
- 7.Departamento de Atención al Público
- 8.Dirección Comercial
- 9.Departamento de Contratos
- 10.Departamento de Control de Usuarios
- 11.Oficina Atención Empresarial
- 12.Dirección de Ingeniería y
- 13.Dirección Operativa.

La Unidad de Transparencia integra este documento de seguridad con base en la información generada por las trece áreas antes señaladas.

1 Consultable en: <http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf>

2 Consultable en: https://www.asechiapas.gob.mx/download/leyes/LEY_PROTECCION_DATOS_PERSONALES.pdf

4. Sistema de gestión de seguridad de los datos personales

El Sistema de Gestión de los Datos Personales constituye el mecanismo mediante el cual el Comité de Agua Potable y Alcantarillado del Municipio de Tapachula (COAPATAP) establece y coordina las acciones necesarias para garantizar la adecuada protección de los datos personales que son tratados en el ejercicio de sus atribuciones, facultades y funciones.

Este sistema comprende las distintas etapas y operaciones relacionadas con el tratamiento de los datos personales, desde su obtención, registro, organización, uso, conservación, acceso, manejo, aprovechamiento, almacenamiento, comunicación, divulgación, transferencia o remisión, hasta su bloqueo, cancelación, supresión, eliminación o destrucción, según corresponda, así como cualquier otra operación vinculada con su tratamiento.

Para tal efecto, el COAPATAP establece políticas, procedimientos, medidas y mecanismos orientados a preservar la confidencialidad, integridad y disponibilidad de los datos personales, en observancia de las disposiciones establecidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas y los Lineamientos aplicables.

Como parte de este proceso, se llevó a cabo una etapa de organización y planeación encaminada a identificar los mecanismos necesarios para la protección de los datos personales. Para ello, se tomaron como punto de partida los procesos, actividades y tareas que desarrollan las diferentes unidades administrativas del COAPATAP en el ejercicio de sus atribuciones y que implican el tratamiento de datos personales.

Con esta finalidad, se establecieron mecanismos para que cada área identificara y documentara los inventarios de datos personales y los sistemas de tratamiento o bases de datos personales que se encuentran bajo su responsabilidad. Para su integración se consideraron, entre otros aspectos, las categorías y tipos de datos personales tratados, incluyendo aquellos que pudieran tener el carácter de sensibles; los medios y mecanismos mediante los cuales son obtenidos; los soportes físicos o electrónicos en los que se encuentran;

Los sistemas utilizados para su acceso, manejo, aprovechamiento, monitoreo y procesamiento; así como las características y condiciones de los espacios en los que se resguardan.

Asimismo, el inventario permite identificar las finalidades de cada tratamiento, las personas servidoras públicas que intervienen o tienen acceso a los datos personales, señalando su nombre, cargo y adscripción, así como, en su caso, las transferencias o remisiones que se realizan, los destinatarios de la información y las razones que justifican dichas operaciones.

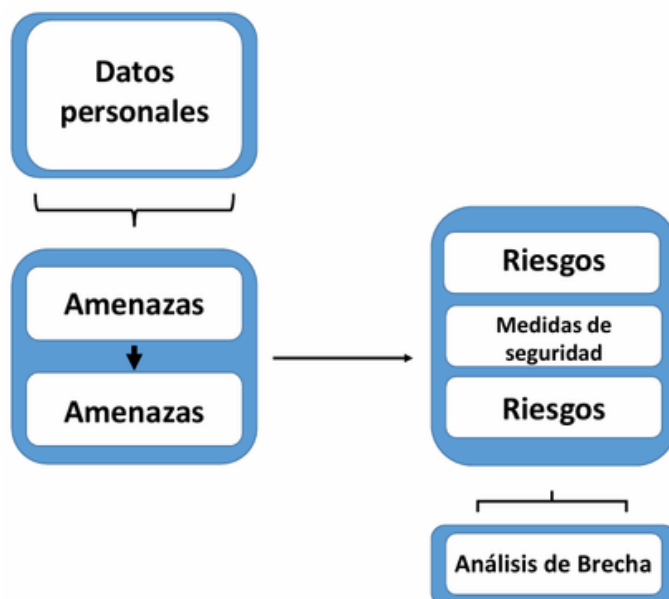
La información obtenida mediante este ejercicio constituye un elemento fundamental para la integración y actualización del inventario de tratamientos de datos personales que forma parte del presente Documento de Seguridad, permitiendo al COAPATAP conocer de manera ordenada los procesos en los que intervienen datos personales y establecer las medidas de seguridad que correspondan de acuerdo con las características y riesgos asociados a cada tratamiento.

De igual manera, el inventario permite considerar el ciclo de vida de los datos personales, desde su obtención hasta la conclusión de la finalidad para la cual fueron recabados. Una vez que dicha finalidad ha sido cumplida y de acuerdo con las disposiciones aplicables, los datos deberán sujetarse a las acciones que correspondan, tales como su bloqueo, cancelación, supresión, eliminación o destrucción.

De igual forma, una vez integrados los inventarios de datos, se dispuso de la metodología para la elaboración del análisis de riesgos, en la cual, 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,¹ las áreas responsables de su tratamiento identificaron el valor de los datos personales de acuerdo con su categoría y el ciclo de vida; el valor de exposición de los activos involucrados en el tratamiento; las consecuencias que pueden generarse para los titulares de los mismos con motivo de su posible vulneración y, los factores de riesgo a los que eventualmente se encuentran expuestos.

¹ Consultable en: https://www.asechiapas.gob.mx/download/leyes/LEY_PROTECCION_DATOS_PERSONALES.pdf

ESQUEMA



La identificación de vulnerabilidades constituye una medida preventiva que permite detectar oportunamente las áreas de oportunidad y las condiciones que pudieran comprometer la seguridad de los datos personales en posesión del COAPATAP, bajo un enfoque proactivo orientado a prevenir posibles incidentes, aun cuando no se haya materializado un daño o afectación.

En este sentido, y con la finalidad de fortalecer las medidas de seguridad implementadas por el Organismo, se consideran de manera enunciativa, más no limitativa, las siguientes posibles vulnerabilidades:

1. Insuficiencia de controles de acceso
2. Manejo inadecuado de datos personales
3. Reproducción no autorizada
4. Destrucción no autorizada
5. Divulgación no autorizada

A partir de la identificación de amenazas y vulnerabilidades, el COAPATAP establece medidas generales de seguridad sujetas a supervisión y mejora continua, mediante políticas y procedimientos institucionales que deberán observar las personas involucradas en el tratamiento de datos personales, actuando en apego a lo establecido en la LGPDPPSO¹ y en la LPDPPSOCHIS,² así como en los Lineamientos.

1 Consultable en: <http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf>

2 Consultable en: https://www.asechiapas.gob.mx/download/leyes/LEY_PROTECCION_DATOS_PERSONALES.pdf

5. Inventario de datos personales y de los sistemas de tratamiento o bases de datos personales

El inventario de tratamientos de datos personales consiste en el registro organizado y documentado de las operaciones que realizan las unidades administrativas que integran el COAPATAP respecto de los datos personales que recaban de las personas, mediante procedimientos físicos o automatizados. Dichas operaciones comprenden desde la obtención, registro, organización, conservación y utilización de los datos, hasta su comunicación, difusión, transferencia, interconexión, rectificación, cancelación y demás actividades relacionadas con su tratamiento, incluyendo aquellas derivadas de la atención de solicitudes para el ejercicio de los derechos de las personas titulares, conforme a las atribuciones de cada área.

Derivado del proceso de recopilación, revisión y actualización de información, y en coordinación con las unidades administrativas del Organismo, se identificó que las distintas áreas que conforman su estructura orgánica realizan actividades que involucran el tratamiento de datos personales, entre las cuales se encuentran:

- Coordinación de Informática.
- Departamento Jurídico.
- Órgano Interno de Control.
- Unidad de Transparencia.
- Departamento de Recursos Humanos.
- Departamento de Recursos Materiales.
- Departamento de Atención al Público.
- Dirección Comercial.
- Departamento de Contratos.
- Departamento de Control de Usuarios.
- Dirección de Ingeniería.
- Dirección Operativa.

Cabe señalar que el tratamiento de datos personales en el COAPATAP deriva del ejercicio de las atribuciones, facultades y funciones que le corresponden como Organismo Operador de los servicios de agua potable y alcantarillado, así como de las actividades administrativas y operativas necesarias para el cumplimiento de sus objetivos institucionales, de conformidad con su Decreto de Creación y demás disposiciones jurídicas aplicables.

En este sentido, las operaciones que implican el tratamiento de datos personales no se limitan a la atención directa de los usuarios de los servicios que proporciona el Organismo, sino que también comprenden actividades relacionadas con la administración de los recursos humanos, materiales y financieros, la prestación de servicios, la gestión documental, los procedimientos jurídicos, la atención de solicitudes de información pública y el cumplimiento de las obligaciones en materia de transparencia y protección de datos personales.

De igual manera, se consideran los tratamientos derivados de la atención de solicitudes para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, así como de portabilidad, cuando resulte aplicable, en términos de la legislación correspondiente.

A partir de la identificación de las actividades desarrolladas por las distintas unidades administrativas, fue posible reconocer los procesos en los que se lleva a cabo algún tratamiento de datos personales. Como resultado de este ejercicio de recopilación y sistematización, se integró el inventario que forma parte del presente Documento de Seguridad, en el cual se describen los tratamientos identificados y se establecen las bases para su clasificación y análisis conforme a sus características, finalidades y operaciones involucradas.

Lo anterior permitirá al COAPATAP contar con un registro estructurado de los tratamientos de datos personales bajo su responsabilidad, así como establecer las medidas de seguridad y acciones de mejora que correspondan, de acuerdo con los riesgos identificados y las disposiciones normativas aplicables.

A partir de lo anterior, el COAPATAP elaboró los inventarios de los distintos tratamientos de datos personales que realizan o efectúan sus áreas, identificando la mayor parte de los elementos informativos que prevén los artículos 50 de la LPDPPSOCHIS¹ y 53 de los Lineamientos, basado en el ciclo de vida de los datos personales, tal como lo requiere el Artículo 54 de dichos Lineamientos. Dichos inventarios forman parte integral del presente documento y se encuentran contenidos en el Anexo No. 1.

¹ Consultable en: https://www.asechiapas.gob.mx/download/leyes/LEY_PROTECCION_DATOS_PERSONALES.pdf

La siguiente tabla muestra un resumen de esos inventarios contenidos en el Anexo No. 1, elaborados por las áreas:

Número de participante	Área, unidad administrativa u órgano administrativo	Número de inventarios	Sistemas de tratamiento o bases de datos personales
1	Coordinación de Informática	2	1. Área de video vigilancia
			2. Portal Institucional y Pago en línea
2	Departamento Jurídico	2	1. Procedimientos administrativos en Materia laboral
			2. Solicitudes de contratos de comodato y convenios en General que se elaboren ante este Organismo
3	Órgano Interno de Control	4	1. Integración de la declaración patrimonial
			2. Quejas y/o denuncias presentadas contra servidores públicos
			3. Sistema de entrega- recepción
			4. Solicitudes de emisión de órdenes de auditoria y verificaciones
4	Unidad de Transparencia	2	1. Atención a su solicitud de acceso a la información pública
			2. Trámite de Acceso, Rectificación, Cancelación, Oposición y Portabilidad (ARCOP) en materia de datos personales
5	Departamento de Recursos Humanos	7	1. Integración de expediente afiliaciones al Seguro Social
			2. Integración del programa de servicio social y prácticas profesionales
			3. Pago de liquidación de jubilados
			4. Pago de retencion de pension alimenticia a pensionadas
			5. Pago retenciones de nómina por concepto de funerarios
			6. Trámites de pago de becas y útiles escolares para los hijos de los trabajadores
			7. Integración de expediente único personal
6	Departamento de Recursos Materiales y Servicios	1	1. Integración del padrón de proveedores y elaboración de contratos de prestación de servicios
7	Departamento de Atención al Público	4	1. Atención a solicitud de apoyo adulto mayor de forma presencial
			2. Atención a solicitud de apoyo cuota ZAP de forma presencial
			3. Atención al público de forma presencial (aclaraciones)
			4. Registro de la Bitácora de entrada de los usuarios a los distintos departamentos de forma presencial

Número de participante	Área, unidad administrativa u órgano administrativo	Número de inventarios	Sistemas de tratamiento o bases de datos personales
8	Dirección Comercial	2	1. Atención de entrega de constancia de no adeudo con contrato
			2. Atención de entrega de constancia de no adeudo sin contrato
9	Departamento de Contratos	2	1. Atención de solicitud de Contrato para nuevos servicios realizada de forma presencial
			2. Atención de Solicitud para cambio de nombre y/o razón social realizada de forma presencial
10	Departamento de Control de Usuarios	7	1. Atención de solicitud de baja definitiva en forma presencial
			2. Atención de solicitud de bajas temporales en forma presencial
			3. Atención de solicitud de fuga en el cuadro de toma en forma presencial
			4. Atención de solicitud de instalación del medidor en forma presencial
			5. Atención de solicitud de reconexión de toma en forma presencial
			6. Atención de solicitud para la verificación de estado de toma en forma presencial
			7. Atención de solicitud para la verificación de material para medidor de forma presencial
11	Oficina Atención Empresarial	2	1. Atención de solicitudes de facturación electrónica realizada y enviada por medio de correo electrónico y/o presencial
			2. Atención para expedición de constancia de factibilidad de trampa de grasas realizada y entregada de manera presencial
12	Dirección de Ingeniería	1	1. Atención de solicitud de Factibilidad de servicios de agua potable, alcantarillado sanitario y alcantarillado pluvial
13	Dirección Operativa	2	1. Atención de usuarios para generar reportes realizados de forma presencial
			2. Atención de usuarios para generar reportes realizados de forma presencial, vía telefónica 073 y vía WhatsApp
Total:		38	

Los tratamientos de datos personales realizados por el COAPATAP se llevan a cabo en estricto cumplimiento de las atribuciones, facultades y funciones establecidas en su Decreto de Creación, así como en las demás disposiciones normativas y administrativas que regulan su funcionamiento. Dichas actividades son desarrolladas por las unidades administrativas a las que les han sido conferidas, con la finalidad de atender los procesos y cumplir con las responsabilidades que corresponden al Organismo.

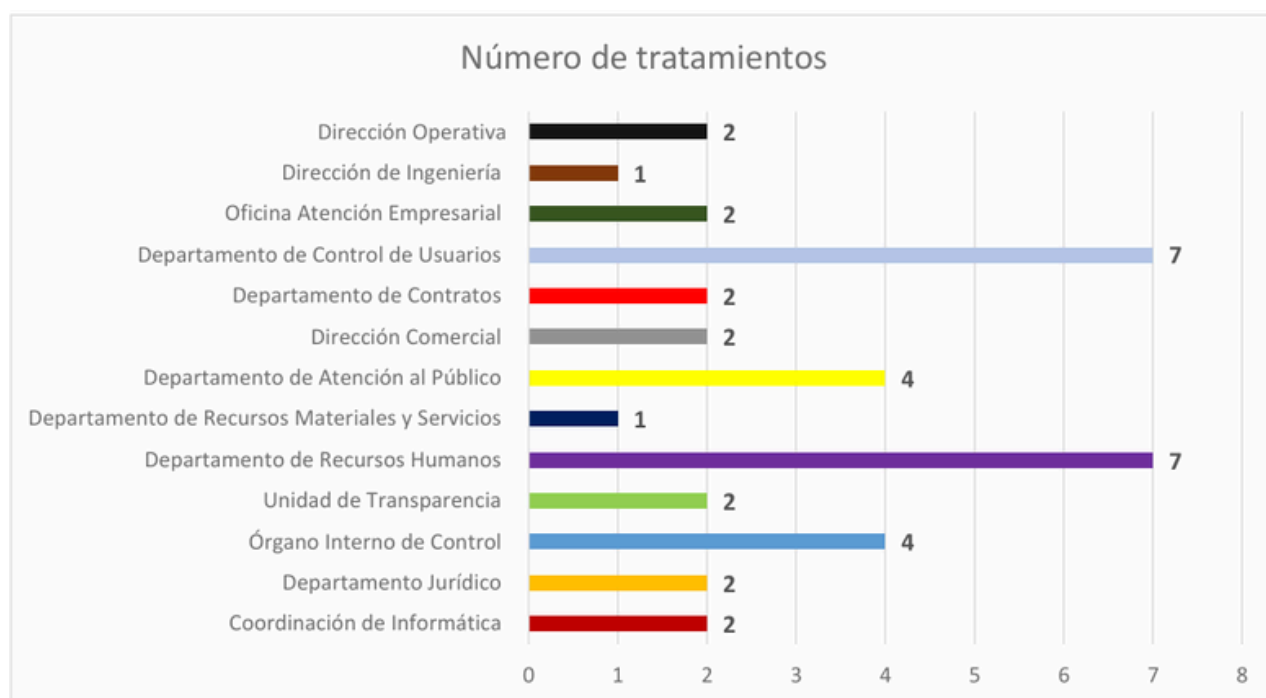
De igual manera, como resultado del análisis efectuado, se identificaron los distintos tipos de datos personales que son objeto de tratamiento, los cuales se agrupan en las siguientes seis categorías:

1. De Identificación: Nombre(s) y apellidos, Sexo, Nacionalidad, Año y/o lugar de nacimiento, Edad, Firma autógrafa o electrónica, Clave Única de Registro de Población (CURP), Registro Federal de Contribuyentes (RFC), Domicilio particular, Número telefónico personal de teléfono fijo o móvil, Correo electrónico personal, Datos personales contenidos en documentos para acreditar la identidad de una persona física, como los contenidos en identificaciones oficiales.
2. Laborales: Experiencia o antecedentes laborales en el sector privado, Puesto en el sector privado, Datos sindicales, Domicilio institucional del trabajo en el sector privado, Número telefónico institucional del trabajo en el sector privado, Correo electrónico institucional del trabajo en el sector privado.
3. Datos académicos: Formación académica, escolaridad o educación, Número de cédula profesional.
4. Patrimoniales: Número de cuenta bancaria, CLABE interbancaria, Descuentos personales.
5. De naturaleza pública: Experiencia o antecedentes laborales en el sector público, Puesto o cargo en el sector público, Domicilio oficial o institucional del empleo, cargo o comisión en el sector público, Número telefónico oficial o institucional del empleo, cargo o comisión en el sector público, Correo electrónico oficial o institucional del empleo, cargo o comisión en el sector público.

6.Sensibles: Afiliación sindical, Tipo de sangre.

7.Otro tipo de datos: Ocupación.

Dichos datos son tratados en 38 procesos, de los cuales dos corresponden a la Coordinación de Informática, dos al Departamento Jurídico, cuatro del Órgano Interno de Control, la Unidad de Transparencia son dos, para el Departamento de Recursos Humanos son tratados siete procesos, uno Departamento de Recursos Materiales, cuatro al Departamento de Atención al Público, dos de Dirección Comercial, Dos del Departamento de Contratos, siete del Departamento de Control de Usuarios, Dos de la Oficina de Atención Empresarial, uno de Dirección de Ingeniería y finalmente dos de Dirección Operativa.

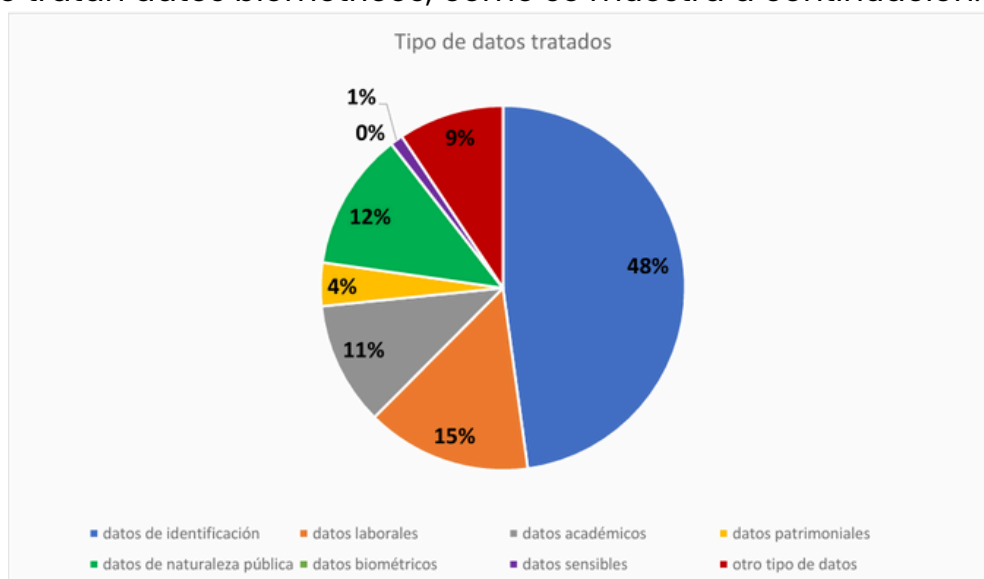


Como se puede apreciar en la gráfica anterior, las áreas con mayor número de procesos son el Departamento de Recursos Humanos y el Departamento de Control de Usuarios con 7 tratamientos cada uno, mientras que las áreas como el Departamento de Recursos Materiales y Servicios y la Dirección de Ingeniería son las que menos procesos desarrolla al ser un solo tratamiento el que realiza o efectúa.

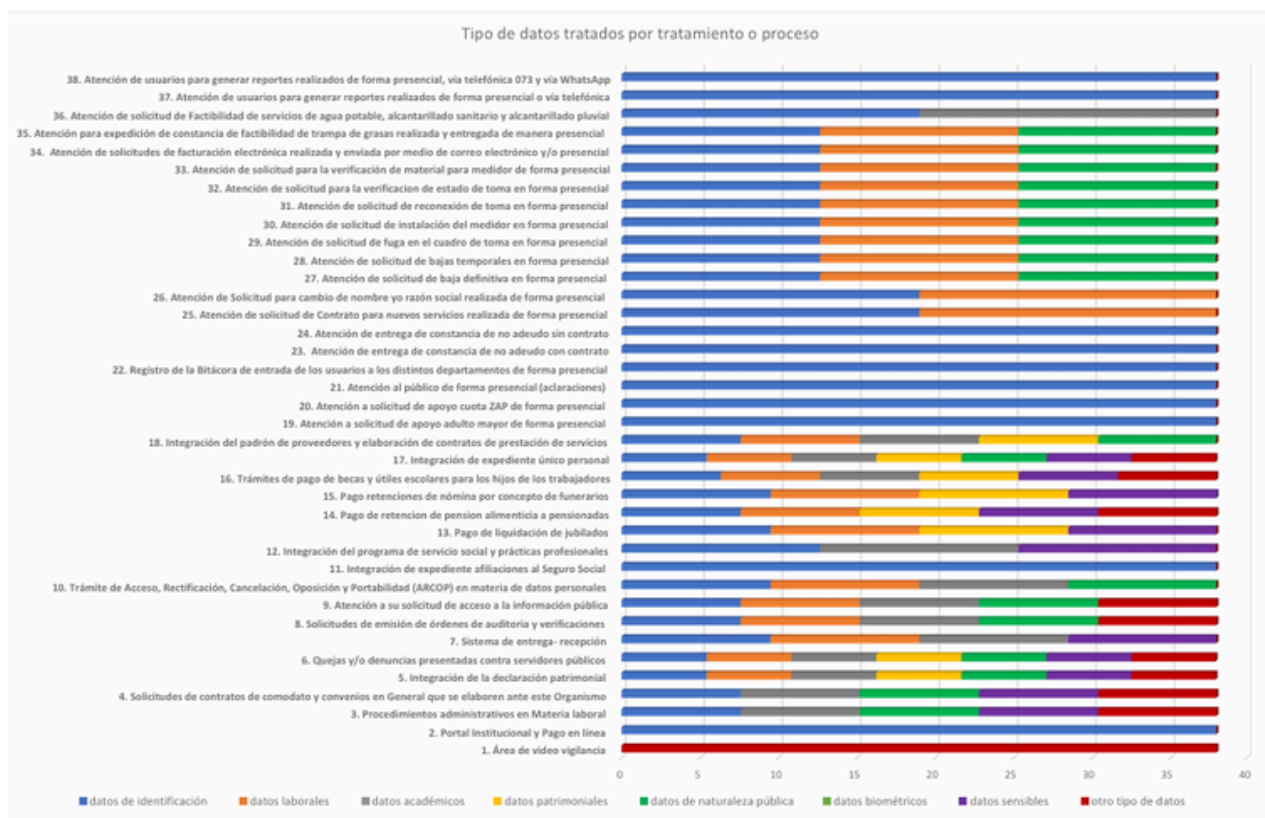
En relación con los datos tratados, todas las áreas recaban datos de identificación, mientras que ninguna de las áreas tratan datos biométricos, tal como se presenta en la siguiente gráfica:



En este sentido, se identificó también que, en relación con los procesos en los que se tratan datos, en el 48 por ciento se tratan datos de identificación, con el 15 por ciento se utilizan los datos laborales, en el 11 por ciento se tratan datos académicos, con el cuatro por ciento se utilizan datos patrimoniales, en el 12 por ciento se tratan datos de naturaleza pública, en el 1 por ciento se tratan datos sensibles, en el 9 por ciento se tratan otro tipo de datos y en el 0 por ciento se tratan datos biométricos; como se muestra a continuación:



Los Departamento de Recursos Humanos y el Departamento de Control de Usuarios son las áreas que desarrolla el mayor número de procesos en los que intervienen tratamientos de datos personales, dada la naturaleza de las atribuciones, facultades o funciones que ejerce, dado de quienes lo integran les compete tratar los datos personales



Los tratamientos de datos personales se realizan principalmente de manera presencial, mediante la comparecencia de las personas titulares, así como a través del correo electrónico y de sistemas electrónicos. Asimismo, cada unidad administrativa desarrolla e implementa estrategias para proteger los datos personales bajo su responsabilidad, mediante la aplicación de las medidas de seguridad correspondientes.

En este contexto, el inventario de datos personales y de los sistemas de tratamiento o bases de datos personales del COAPATAP constituye un componente fundamental de su Sistema de Gestión de Datos Personales, ya que permite identificar las necesidades de protección y establecer, en conjunto con las medidas de seguridad, las acciones necesarias para garantizar el adecuado tratamiento de la información personal.

De igual manera, dicho inventario permite identificar las necesidades de capacitación de las personas servidoras públicas del Organismo, contribuyendo al fortalecimiento de los procesos en los que se tratan datos personales y promoviendo la sensibilización y preparación del personal responsable, a fin de que sus actividades se desarrollen conforme a las disposiciones y estándares aplicables en la materia.

El inventario de datos personales y de los sistemas de tratamiento o bases de datos personales del COAPATAP se consolida como un elemento más de la política implementada para la observancia de la LGPDPPSO, de la LPDPPSOCHIS y de los Lineamientos, dando certeza a todas las personas titulares de los datos personales sobre el destino de sus datos recabados por este Sujeto Obligado.

6. Funciones y Obligaciones de las personas que tratan datos personales

Derivado de la identificación de los procesos que involucran el tratamiento de datos personales, mismos que se encuentran documentados en el Inventario de Datos Personales, resulta necesario vincular dichas actividades con las atribuciones, facultades y funciones establecidas en la normativa interna del COAPATAP, las cuales confieren a las personas servidoras públicas la responsabilidad de llevar a cabo dichos tratamientos.

Lo anterior, con la finalidad de garantizar que el tratamiento de datos personales se realice en estricto apego al principio de legalidad que rige la actuación de las personas servidoras públicas.

En este sentido, a continuación, se describen las funciones y atribuciones conferidas a las unidades administrativas del COAPATAP, en virtud de las cuales se realizan tratamientos de datos personales.

Área, unidad administrativa u órgano administrativo	Nombre y Cargo de las personas Servidoras Públicas que tratan los Datos Personales	Sistemas de tratamiento o bases de datos personales
Coordinación de Informática	Ing. Mauricio de Jesús Ochoa Luis, Coordinador de Informática, Ing. José Agustín paz Montalvo, Ing. Iván marco Rodríguez TorcyWinkler, Auxiliar de Informática, C. Osmar Zaratt Rincón Cisneros, Auxiliar de Informática.	1. Área de video vigilancia
		2. Portal Institucional y Pago en línea
Departamento Jurídico	Lic. Carlos Calderón Ordóñez, Jefe del Departamento Jurídico, Lic. Ramón Sánchez Zavala, Asesor Jurídico, Lic. Alexander Coutiño González, Asesor Jurídico.	1. Procedimientos administrativos en Materia laboral
		2. Solicitudes de contratos de comodato y convenios en General que se elaboren ante este Organismo
Órgano Interno de Control	C.P. Carlos Alberto García Marín, Titular del Órgano Interno de Control, C.P. David Victorio Domínguez, Coordinador de Auditorías, C.P. Pedro Gabriel Cruz Pérez, Auditor Interno, Lic. Ingrid Denned López Vázquez, Jefa del Departamento de Investigación, Lic. Xitlali del Carmen Hernández López, Auxiliar administrativo, Lic. Romeo Aguilar López, Auxiliar Administrativo.	1. Integración de la declaración patrimonial
		2. Quejas y/o denuncias presentadas contra servidores públicos
		3. Sistema de entrega- recepción
		4. Solicitudes de emisión de órdenes de auditoria y verificaciones

Área, unidad administrativa u órgano administrativo	Nombre y Cargo de las personas Servidoras Públicas que tratan los Datos Personales	Sistemas de tratamiento o bases de datos personales
Unidad de Transparencia	Mtra. Arantza Cueto Jiménez, Jefa Oficina de Archivo y Transparencia	1. Atención a su solicitud de acceso a la información pública
		2. Trámite de Acceso, Rectificación, Cancelación, Oposición y Portabilidad (ARCOP) en materia de datos personales
Departamento de Recursos Humanos	Mtra. Karla Verónica Castañeda Trujillo, Jefa del Departamento de Recursos Humanos, Lic. Frida Guadalupe Moreno Cisneros, Auxiliar Administrativo, C.P. Martha del Rocio Martínez Hernández, Auxiliar Administrativo, C.P. José Otilio Wong Cruz, Auxiliar Administrativo, C.P. Francisco Adie Vera Cisneros, Auxiliar Administrativo, C.P. Elí Fernando Ramírez Dardon, Auxiliar Administrativo, C. Francisco Javier Carbajal Roblero, Auxiliar Administrativo, Lic. Alejandra Victoria Chacón Solís, Auxiliar Administrativo, C.P. Heriberto Mejía Orellana, Auxiliar Administrativo, Lic. Claudia Karina Villalobos López.	1. Integración de expediente afiliaciones al Seguro Social
		2. Integración del programa de servicio social y prácticas profesionales
		3. Pago de liquidación de jubilados
		4. Pago de retención de pensión alimenticia a pensionadas
		5. Pago retenciones de nómina por concepto de funerarios
		6. Trámites de pago de becas y útiles escolares para los hijos de los trabajadores
		7. Integración de expediente único personal
Departamento de Recursos Materiales y Servicios	Lic. Carlos Alberto Martínez Ortega, Jefe del Departamento de Recursos Materiales y Servicios, Ing. Sergio Hiram Torres Monzón, jefe de oficina de adquisiciones y licitaciones, L.C.I Daniella García Pimentel, Auxiliar Administrativo	1. Integración del padrón de proveedores y elaboración de contratos de prestación de servicios
Departamento de Atención al Público	C. Nery Flor López Arrevillaga, Jefa del Departamento Atención al Público, C. Jaqueline Cortez de León, Auxiliar Administrativo, C. Anabeli Ruiz Cárdenas, Auxiliar Administrativo, C. Reyna del Carmen Enríquez Velázquez, Auxiliar Administrativo, c. Mercedes Ordoñez Muñoz, Auxiliar Administrativo, c. Rosario Chacón Santiago, Auxiliar Administrativo	1. Atención a solicitud de apoyo adulto mayor de forma presencial
		2. Atención a solicitud de apoyo cuota ZAP de forma presencial
		3. Atención al público de forma presencial (acleraciones)
		4. Registro de la Bitácora de entrada de los usuarios a los distintos departamentos de forma presencial
Dirección Comercial	C.P. Rocio Liliana Ovando Trujillo, Directora Comercial, C. Margarita Cristel Fernández Zetina, Auxiliar Administrativo	1. Atención de entrega de constancia de no adeudo con contrato
		2. Atención de entrega de constancia de no adeudo sin contrato

Área, unidad administrativa u órgano administrativo	Nombre y Cargo de las personas Servidoras Públicas que tratan los Datos Personales	Sistemas de tratamiento o bases de datos personales
Departamento de Contratos	C. Diana Rosa Contreras López, Jefa Depto. de Contratos, C. Elubia Roblero Sala, Auxiliar Administrativo, C. Aurora Angélica D'Amiano Sumuano, Auxiliar Administrativo, c. Marliss Olinka López Hernández, Auxiliar Administrativo, c. Luis Guadalupe Escobar Méndez, Auxiliar Administrativo, c. Liliana Rodas Caballero, Auxiliar Administrativo, Lic. Araceli López Díaz, Auxiliar Administrativo, Lic. Lorena Galindo Anguiano, Auxiliar Administrativo, C. Lucila Domínguez Ramírez, Auxiliar Administrativo, c. Martin Romeo Rosales Castañeda, Auxiliar Administrativo.	1. Atención de solicitud de Contrato para nuevos servicios realizada de forma presencial
		2. Atención de Solicitud para cambio de nombre y/o razón social realizada de forma presencial
Departamento de Control de Usuarios	C. Rafael Morales Alcabala, Jefe Departamento de Control de Usuarios, C. Francisca Arguello Hernández, Auxiliar Administrativo, Lic. Alicia del Rosario Hernández Torres, Auxiliar Administrativo, C. Lizbeth Alejandra Herrera Ruiz, Auxiliar Administrativo, C. Francisco Matías Hernández, Jefe de Cuadrilla, C. Mario Antonio Hernández Domínguez, Jefe de Cuadrilla, C. José Manuel Arguello Hernández, Jefe de Cuadrilla.	1. Atención de solicitud de baja definitiva en forma presencial
		2. Atención de solicitud de bajas temporales en forma presencial
		3. Atención de solicitud de fuga en el cuadro de toma en forma
		4. Atención de solicitud de instalación del medidor en forma
		5. Atención de solicitud de reconexión de toma en forma
		6. Atención de solicitud para la verificación de estado de toma en forma presencial
		7. Atención de solicitud para la verificación de material para medidor de forma presencial
Oficina Atención Empresarial	Mtra. Dulce Karolina García Bravo, Jefa Oficina Atención Empresarial, Lic. Ana Laura López de León, Auxiliar Administrativo "B", Lic. Adrián Rueda Gómez, Auxiliar Administrativo "B", C.P. Sandra Carolina Aguilar Domínguez, Auxiliar Administrativo "A".	1. Atención de solicitudes de facturación electrónica realizada y enviada por medio de correo electrónico y/o presencial
		2. Atención para expedición de constancia de factibilidad de trampa de grasas realizada y entregada de manera presencial
Dirección de Ingeniería	Ing. Juan Antonio Ruvalcaba Contreras, Director de Ingeniería, Lic. Alicia Rodas Moreno, Asistente Dirección de Ingeniería.	1. Atención de solicitud de Factibilidad de servicios de agua potable, alcantarillado sanitario y alcantarillado pluvial
Dirección Operativa	Ing. Claudia Alejandra Chool Roblero, Directora Operativa, C. Esperanza de Jesús Lázaro Sánchez, Auxiliar Administrativo, Lic. Alexis Michelle Juárez Mota, Auxiliar Administrativo, Lic. Gilberto Meza Catalán, Atención al Público, Ing. Estelita López Santiago, Atención 073.	1. Atención de usuarios para generar reportes realizados de forma presencial o vía telefónica
		2. Atención de usuarios para generar reportes realizados de forma presencial, vía telefónica 073 y vía WhatsApp

7. Análisis de Riesgos y de Brecha

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

Se testea el apartado núm. 7, que contiene el Análisis de Riesgo y 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 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 testea el apartado núm. 7, que contiene el Análisis de Riesgo y 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 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 testea el apartado núm. 7, que contiene el Análisis de Riesgo y 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 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 testea el apartado núm. 7, que contiene el Análisis de Riesgo y 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 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 testea el apartado núm. 7, que contiene el Análisis de Riesgo y 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 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 testea el apartado núm. 7, que contiene el Análisis de Riesgo y 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 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 testea el apartado núm. 7, que contiene el Análisis de Riesgo y 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 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 testea el apartado núm. 7, que contiene el Análisis de Riesgo y 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 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 testea el apartado núm. 7, que contiene el Análisis de Riesgo y 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 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 testea el apartado núm. 7, que contiene el Análisis de Riesgo y 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 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.

8. Gestión de Vulneraciones y Plan de Contingencia

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

Se testea el apartado núm. 8, 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 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 testea el apartado núm. 8, 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 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 testea el apartado núm. 8, 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 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 testea el apartado núm. 8, 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 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 testea el apartado núm. 8, 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 y desclasificación de la información, así como para la elaboración de versiones públicas.

9. Medidas de Seguridad Generales

Las medidas generales de seguridad administrativas, físicas y técnicas implementadas actualmente por el COAPATAP tienen como finalidad preservar la confidencialidad e integridad de la información, así como prevenir daños, pérdidas, destrucción o alteración de los datos personales, evitando su uso, acceso, tratamiento o divulgación sin la debida autorización.

9.1 Medidas administrativas

Constituyen el conjunto de políticas, procedimientos, controles, mecanismos y acciones de carácter organizacional orientados a asegurar que el tratamiento de los datos personales se lleve a cabo en apego a las disposiciones normativas aplicables, así como a prevenir, detectar y atender posibles vulneraciones de seguridad.

No.	Medidas de Seguridad	Responsable	Periodicidad
1	Implementar formatos de control para el préstamo y devolución de documentos, a cargo del área responsable del archivo.	Oficina de Archivo / Área responsable del expediente	Cada vez que se realice un préstamo o devolución
2	Garantizar el resguardo y conservación de los expedientes, conforme a la normativa archivística aplicable.	Oficina de Archivo y responsables de los archivos de trámite	Permanente
3	Establecer y mantener mecanismos de control documental, conforme a las disposiciones del Sistema de Gestión Documental del COAPATAP.	Oficina de Archivo / Responsables de archivo de trámite	Permanente y revisión anual
4	Informar al superior jerárquico sobre incidentes relacionados con la pérdida, extravío, alteración o afectación de documentos que contengan datos personales.	Persona servidora pública que detecte el incidente / Titular del área/Órgano Interno de Control	Permanente y revisión anual
5	Capacitar y sensibilizar al personal en materia de protección de datos personales y seguridad de la información.	Unidad de Transparencia / Departamento de Recursos Humanos	Al menos una vez al año y cuando resulte necesario

No.	Medidas de Seguridad	Responsable	Periodicidad
6	Establecer procedimientos para el alta, modificación, actualización y baja de usuarios y permisos de acceso a los sistemas de tratamiento.	Coordinación de Informática / Titulares de las áreas	Cada vez que exista alta, cambio de funciones o baja de personal
7	Realizar análisis de riesgos y evaluaciones de las medidas de seguridad implementadas.	Unidad de Transparencia / Coordinación de Informática / Titulares de las áreas	Al menos una vez al año y cuando existan cambios relevantes
8	Implementar un procedimiento para la gestión de incidentes y vulneraciones de seguridad, incluyendo su registro, atención, documentación y seguimiento.	Unidad de Transparencia / Coordinación de Informática / Área involucrada	Cada vez que se presente un incidente o vulneración
9	Realizar revisiones para verificar el cumplimiento de las políticas, procedimientos y controles de seguridad.	Comité de Transparencia / Unidad de Transparencia / Titulares de las áreas	Al menos una vez al año
10	Implementar acciones preventivas y correctivas derivadas de revisiones, evaluaciones, incidentes o vulneraciones de seguridad.	Titular del área involucrada / Unidad de Transparencia / Coordinación de Informática, según corresponda	Conforme a los resultados de cada revisión o incidente
11	Realizar reuniones de seguimiento para evaluar la eficacia de las medidas implementadas y promover la mejora continua.	Comité de Transparencia / Unidad de Transparencia / Áreas involucradas	Semestral y cuando resulte necesario
12	Dar vista al Órgano Interno de Control cuando se identifiquen hechos u omisiones que pudieran constituir responsabilidades administrativas relacionadas con una vulneración de datos personales.	Titular del área involucrada / Unidad de Transparencia	Cuando se identifiquen hechos u omisiones que pudieran generar responsabilidad administrativa

9.2 Medidas físicas

Constituyen el conjunto de políticas, procedimientos, controles, mecanismos y acciones de carácter organizacional orientados a asegurar que el tratamiento de los datos personales se lleve a cabo en apego a las disposiciones normativas aplicables, así como a prevenir, detectar y atender posibles vulneraciones de seguridad.

No.	Medidas de Seguridad	Responsable	Periodicidad
1	Resguardar los documentos y expedientes que contengan datos personales en los archivos de trámite y de concentración, conforme a las disposiciones archivísticas aplicables.	Responsables de Archivo de Trámite y Archivo de Concentración	Permanente
2	Llevar una bitácora de acceso al Archivo de Concentración para identificar a las personas que ingresan, su área de adscripción y motivo de acceso.	Responsable del Archivo de Concentración	Cada vez que se registre un acceso
3	Mantener mecanismos físicos de control de acceso, como chapas, cerraduras y llaves, en las áreas destinadas al resguardo de información.	Titular del área / Oficina de Activo Fijo	Permanente; revisión semestral
4	Restringir el acceso a los archivos físicos únicamente al personal autorizado que requiera consultar o manipular los expedientes.	Titular del área / Responsable del archivo	Permanente; revisión anual de autorizaciones
5	Mantener sistemas de videovigilancia (CCTV), cuando corresponda, para contribuir al control de accesos y vigilancia de las áreas restringidas.	Coordinación de Informática / Área responsable de Seguridad o Vigilancia	Monitoreo permanente; revisión periódica
6	Aplicar la política de escritorios limpios, retirando y resguardando al término de la jornada los documentos, expedientes y dispositivos que contengan datos personales.	Todo el personal que trate datos personales / Titulares de las áreas	Diaria

No.	Medidas de Seguridad	Responsable	Periodicidad
7	Mantener libres de documentos que contengan datos personales las impresoras, escáneres y demás equipos de reproducción.	Personal del Organismo/ Titulares de las áreas	Permanente; verificación diaria
8	Contar con extintores y demás elementos de protección contra incendios en las áreas donde se resguarde documentación o soportes con datos personales.	Área Administrativa / Responsable de Protección Civil	Revisión periódica conforme al programa institucional
9	Aplicar procedimientos de borrado seguro de información contenida en equipos y medios de almacenamiento antes de su reutilización, reasignación, mantenimiento, baja o disposición final.	Coordinación de Informática / Área responsable del equipo	Cada vez que un equipo o medio sea reutilizado, reasignado o dado de baja
10	Realizar mantenimiento preventivo y respaldos periódicos de los equipos y sistemas que contengan información institucional.	Coordinación de Informática	Conforme al programa de mantenimiento y respaldo institucional
11	Reportar inmediatamente cualquier pérdida, extravío, robo, daño o acceso no autorizado relacionado con equipos, documentos, expedientes o soportes que contengan datos personales.	Persona servidora pública que detecte el incidente / Titular del área	Inmediata, al detectar el incidente

9.3 Medidas técnicas

Son las medidas y mecanismos tecnológicos establecidos para proteger los sistemas de tratamiento, equipos, redes y demás recursos informáticos que intervienen en el manejo de datos personales, con la finalidad de garantizar su confidencialidad, integridad y disponibilidad, así como prevenir accesos, alteraciones, pérdidas, daños o divulgaciones que no cuenten con la debida autorización.

9.3 Medidas técnicas

No.	Medidas de Seguridad	Responsable	Periodicidad
1	Administración de cuentas y privilegios de acceso. Establecer y mantener un esquema de asignación de permisos basado en roles y funciones, de manera que cada persona servidora pública tenga únicamente los privilegios necesarios para desempeñar sus actividades, aplicando los principios de mínimo privilegio y necesidad de conocer.	Coordinación de Informática, en conjunto con las personas responsables de cada área.	Semestral y cada vez que exista un cambio de funciones, puesto o área.
2	Protección de credenciales de acceso. Las personas usuarias deberán mantener bajo resguardo sus nombres de usuario y contraseñas, evitando compartirlas o permitir que terceros hagan uso de ellas. En caso de detectar, sospechar o identificar un uso no autorizado, deberán reportarlo inmediatamente al Área de Informática para realizar las acciones de protección correspondientes.	Personas usuarias y Área de Informática.	Permanente; atención inmediata ante cualquier incidente.
3	Uso institucional del correo electrónico. Utilizar las cuentas de correo electrónico institucional exclusivamente para el desarrollo de actividades laborales y evitar el envío de datos personales, salvo que exista una necesidad justificada y se implementen las medidas de seguridad correspondientes para proteger la información.	Personas servidoras públicas usuarias del correo institucional.	Permanente
4	Resguardo y protección de archivos electrónicos. Mantener los documentos y archivos electrónicos que contengan datos personales en equipos, servidores, sistemas o repositorios institucionales autorizados, evitando su almacenamiento en dispositivos o ubicaciones no autorizadas. Cuando corresponda, deberán aplicarse mecanismos de protección como cifrado, contraseñas o restricciones de acceso.	Personas responsables de las áreas y Coordinación de Informática.	Permanente, con revisión semestral de los permisos de acceso.

9.3 Medidas técnicas

No.	Medidas de Seguridad	Responsable	Periodicidad
5	Control en la transferencia y distribución de información. Evitar la difusión, transmisión, descarga o intercambio de documentos electrónicos que contengan datos personales con personas no autorizadas. Previamente a compartir información, deberá verificarse que la persona destinataria cuente con autorización y que el medio utilizado sea institucional y seguro.	Personas servidoras públicas que realizan el tratamiento de datos personales y responsables de área.	Permanente
6	Revocación de accesos por baja o cambio de funciones. Las personas responsables de las áreas deberán informar oportunamente al Área de Informática sobre las bajas, cambios de adscripción, puesto o funciones del personal que tenga acceso a sistemas o información que contenga datos personales, a efecto de cancelar, modificar o restringir los permisos correspondientes.	Dirección Administrativa, Departamento de Recursos Humanos y Coordinación de Informática.	Inmediata, al presentarse la baja o modificación de funciones.
7	Actualización y mantenimiento de software. La instalación, actualización, configuración y mantenimiento de programas, sistemas operativos, aplicaciones y demás software utilizado en los equipos institucionales será realizada exclusivamente por el Área de Informática, a fin de reducir riesgos derivados del uso de programas no autorizados o desactualizados.	Coordinación de Informática.	Periódica, de acuerdo con las necesidades técnicas, actualizaciones disponibles y políticas institucionales; así como inmediata cuando se identifique una vulnerabilidad crítica.

10. Plan de Trabajo

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

Se testea el apartado núm. 10 que contiene el Plan de Trabajo, en virtud de ser un instrumento de gestión que deriva del análisis de riesgo y del análisis de brecha, en el se establecen las acciones específicas que el Sujeto Obligado implementará para corregir deficiencias, fortalecer controles y reducir los riesgos identificados, cuya divulgación podría comprometer la seguridad del sistema de tratamiento de datos personales, 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 testea el apartado núm. 10 que contiene el Plan de Trabajo, en virtud de ser un instrumento de gestión que deriva del análisis de riesgo y del análisis de brecha, en el se establecen las acciones específicas que el Sujeto Obligado implementará para corregir deficiencias, fortalecer controles y reducir los riesgos identificados, cuya divulgación podría comprometer la seguridad del sistema de tratamiento de datos personales, 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 testea el apartado núm. 10 que contiene el Plan de Trabajo, en virtud de ser un instrumento de gestión que deriva del análisis de riesgo y del análisis de brecha, en el se establecen las acciones específicas que el Sujeto Obligado implementará para corregir deficiencias, fortalecer controles y reducir los riesgos identificados, cuya divulgación podría comprometer la seguridad del sistema de tratamiento de datos personales, 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 testea el apartado núm. 10 que contiene el Plan de Trabajo, en virtud de ser un instrumento de gestión que deriva del análisis de riesgo y del análisis de brecha, en el se establecen las acciones específicas que el Sujeto Obligado implementará para corregir deficiencias, fortalecer controles y reducir los riesgos identificados, cuya divulgación podría comprometer la seguridad del sistema de tratamiento de datos personales, 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 testea el apartado núm. 10 que contiene el Plan de Trabajo, en virtud de ser un instrumento de gestión que deriva del análisis de riesgo y del análisis de brecha, en el se establecen las acciones específicas que el Sujeto Obligado implementará para corregir deficiencias, fortalecer controles y reducir los riesgos identificados, cuya divulgación podría comprometer la seguridad del sistema de tratamiento de datos personales, 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.

11. Propuesta de Capacitación en Materia de Datos Personales

La formación y actualización del personal representan elementos necesarios para consolidar las acciones institucionales encaminadas a la protección de los datos personales. A través de actividades de capacitación, se busca que las personas servidoras públicas que intervienen en el tratamiento de información conozcan sus responsabilidades, identifiquen los riesgos asociados a su manejo y apliquen correctamente los controles y medidas de seguridad establecidos por el Organismo.

La preparación permanente del personal permite reforzar las prácticas relacionadas con el manejo, resguardo y protección de los datos personales, así como favorecer la correcta aplicación de las medidas de seguridad administrativas, físicas y técnicas implementadas. Asimismo, contribuye a mantener actualizados los sistemas e inventarios de tratamiento, prevenir posibles incidentes y asegurar que las actividades realizadas por el personal se desarrollen conforme a los principios, deberes y obligaciones establecidos en la normativa aplicable.

Para tal efecto, el Organismo contempla el desarrollo de un Programa Institucional de Capacitación en Materia de Protección de Datos Personales, dirigido al personal que, derivado de las funciones inherentes a su puesto, tenga contacto, acceso o intervenga de cualquier manera en el tratamiento de datos personales.

El programa estará orientado a proporcionar herramientas prácticas y conocimientos normativos que permitan al personal desempeñar sus actividades de manera segura y responsable. De igual forma, buscará unificar criterios para la identificación de riesgos, aplicación de medidas de seguridad, atención de situaciones que puedan comprometer la información y cumplimiento de las obligaciones institucionales en materia de protección de datos personales.

Las actividades de capacitación podrán desarrollarse mediante cursos, talleres, pláticas, sesiones informativas, materiales de difusión y demás mecanismos que resulten adecuados para las necesidades del Organismo. Los contenidos serán determinados considerando las funciones del personal, los sistemas de tratamiento existentes, los riesgos identificados y las modificaciones que se presenten en la normativa aplicable.

De manera enunciativa, mas no limitativa, se podrán considerar los siguientes temas:

- **Introducción al derecho a la protección de datos personales**

1. Marco conceptual.
2. Principios aplicables al tratamiento de datos personales.
3. Deberes de los sujetos obligados.
4. Sistemas de tratamiento de datos personales.
5. Medidas de seguridad administrativas, físicas y técnicas.
6. Derechos ARCO (Acceso, Rectificación, Cancelación y Oposición).
7. Procedimientos de tutela, medios de impugnación y régimen de responsabilidades.

- **Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas¹**

1. Antecedentes y evolución normativa.
2. Ámbito de aplicación.
3. Objeto y finalidad de la Ley.
4. Principales obligaciones de los sujetos obligados.
5. Responsabilidades y consecuencias derivadas del incumplimiento.

- **Programa Institucional de Protección de Datos Personales**

1. Sistemas de tratamiento de datos personales.
2. Inventario de datos personales y bases de datos.
3. Documento de Seguridad.
4. Medidas de seguridad administrativas, físicas y técnicas.
5. Análisis de brecha y análisis de riesgos.
6. Funciones y responsabilidades de las personas servidoras públicas que intervienen en el tratamiento de datos personales.
7. Acciones de monitoreo, supervisión y mejora continua del Sistema de Gestión de Seguridad de Datos Personales.

¹ Consultable en: https://www.asechiapas.gob.mx/download/leyes/LEY_PROTECCION_DATOS_PERSONALES.pdf



Conciencia sobre el Agua

Documento de Seguridad

Sistema de Datos Personales del Comité de Agua Potable y Alcantarillado del Municipio de Tapachula

	Fecha de elaboración del Documento de Seguridad: 17 de septiembre de 2026	Fecha de última actualización del Documento de Seguridad: 30 de septiembre de 2026
	Elaboró:	Aprobó
	Mtra. Arantza Cueto Jiménez, Unidad de Transparencia	Lic. Héctor Manuel Lazos Cota, Director General del COAPATAP

Unidad de Transparencia

Correo Electrónico:
transparencia@coapatap.gob.mx