

COMITÉ DE AGUA POTABLE Y ALCANTARILLADO MUNICIPAL DE COMITÁN DE DOMÍNGUEZ, CHIAPAS (COAPAM)

DOCUMENTO DE SEGURIDAD EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

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

Control documental	Dato
Sujeto obligado	COAPAM – Comité de Agua Potable y Alcantarillado Municipal de Comitán de Domínguez, Chiapas
Documento	Documento de Seguridad en materia de Protección de Datos Personales
Fecha de emisión	Septiembre de 2026
Vigencia	A partir de su aprobación y hasta su actualización
Responsable de coordinación	Unidad de Transparencia / área competente en protección de datos personales
Aprobación	Comité de Transparencia de COAPAM
Clasificación de trabajo	Documento de uso institucional y acceso restringido en lo relativo a controles de seguridad

“Documento sujeto a revisión, validación y aprobación por las instancias competentes de COAPAM.”

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



1. PRESENTACIÓN

El comité de agua potable y alcantarillado municipal, en cumplimiento de sus responsabilidades institucionales y con el propósito de fortalecer la confianza de la ciudadanía, establece el presente documento en materia de seguridad de la información y protección de datos personales.

La prestación de los servicios de agua potable, alcantarillado y saneamiento implica la generación, recepción, conservación y tratamiento de información de carácter administrativo, técnico, financiero y personal de las personas usuarias, trabajadores, proveedores y demás personal relacionadas con el organismo.

En este sentido, resulta indispensable establecer medidas que permitan prevenir, identificar y atender riesgos de seguridad, así como garantizar que los datos personales sean tratados de manera lícita, segura, confidencial y exclusivamente para las finalidades institucionales que correspondan.

El presente documento tiene como finalidad establecer criterios, responsabilidades y medidas de carácter administrativo, técnico y físico para proteger la información que se encuentra bajo resguardo del comité, procurando preservar su confidencialidad, integridad y disponibilidad.

Así mismo, busca promover una cultura institucional de protección de la información entre las personas servidoras públicas, estableciendo buenas prácticas para el manejo de expedientes, sistemas informáticos, documentos físicos, bases de datos, contraseñas, equipos de cómputo y demás recursos que contengan información institucional o datos personales.

La aplicación de estas disposiciones deberá observar en todo momento el marco jurídico aplicable en materia de protección de datos personales, archivos, transparencia, seguridad de la información y responsabilidades administrativas, así como los principios y deberes que correspondan al comité como sujeto obligado.

Con este instrumento, el comité reafirma su compromiso con una gestión responsable de la información, la protección de los derechos de las personas y el fortalecimiento de una administración pública eficiente, transparente y segura.



El presente Documento de Seguridad establece las medidas administrativas, físicas y técnicas que deberán observarse para proteger los datos personales que sean tratados por el Comité de Agua Potable y Alcantarillado Municipal de Comitán de Domínguez, Chiapas (COAPAM), en el ejercicio de sus atribuciones.

El documento considera de manera transversal a la Unidad de Transparencia y a las Coordinaciones Operativa, Comercial, Administrativa y de Cultura del Agua. Su finalidad es establecer controles proporcionales al riesgo para preservar la confidencialidad, integridad y disponibilidad de los datos personales.

Este instrumento deberá aplicarse durante todo el ciclo de vida del dato: obtención, uso, registro, organización, conservación, consulta, comunicación, transferencia, bloqueo cuando corresponda y supresión, conforme a las disposiciones jurídicas aplicables y a las determinaciones institucionales de COAPAM.

2. OBJETIVO

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

Establecer un marco institucional para identificar, administrar, proteger y supervisar los tratamientos de datos personales realizados por COAPAM, mediante controles que reduzcan riesgos de pérdida, destrucción, robo, extravío, copia, acceso, uso, tratamiento, alteración o modificación no autorizados.

- Identificar los tratamientos y sistemas en los que se manejan datos personales.
- Definir funciones y obligaciones de las personas servidoras públicas que intervienen en dichos tratamientos.
- Implementar medidas administrativas, físicas y técnicas acordes con el riesgo.
- Establecer mecanismos para prevenir, detectar, atender y documentar vulneraciones de seguridad. **ACCESOS, USOS, MODIFICACIONES, PÉRDIDAS O DIVULGACIONES NO AUTORIZADAS**

- Establecer un programa de capacitación y mejora continua.
- Facilitar la atención de los derechos de las personas titulares y la coordinación con la Unidad de Transparencia.
- Proteger la información de usuarios, trabajadores, proveedores y demás personas relacionadas con el Comité.
- Establecer procedimientos para atender incidentes de seguridad que involucren datos personales.

2. ALCANCE

El presente Documento de Seguridad es aplicable a todas las personas servidoras públicas, personal eventual, prestadores de servicios y terceros que, por sus funciones o mediante un encargo autorizado, intervengan en el tratamiento de datos personales bajo responsabilidad de COAPAM.

Área	Tratamientos principales que deberán identificarse y documentarse
Unidad de Transparencia	Solicitudes de acceso a datos personales y derechos ARCO; integración de expedientes; avisos de privacidad; gestión de incidentes; coordinación con áreas.
Coordinación Operativa	Órdenes de trabajo, reportes de servicios, inspecciones, visitas, atención de fugas, tomas, domicilios, fotografías y datos de contacto cuando sean identificables. Atención de fugas de agua y drenaje.
Coordinación Comercial	Contratos y cuentas de usuarios, altas/bajas, convenios, adeudos, aclaraciones, cambio de nombre, restricción de service de agua potable, multas por desperdicio de agua, domicilios, teléfonos, correos y documentos de acreditación de la propiedad.
Coordinación Administrativa	Expedientes de personal, nómina, proveedores, contrataciones, pagos,



	viáticos, controles de asistencia y documentación administrativa que contenga datos personales. Facturación, correos electrónicos.
Coordinación de Cultura del Agua	Registros de participantes, escuelas, docentes, imágenes, actividades y datos de contacto.

3. MARCO JURÍDICO

El documento se formula con base en el marco vigente al momento de su elaboración, entre otros ordenamientos aplicables:

- Constitución Política de los Estados Unidos Mexicanos, en su artículo 16, en materia de protección de datos personales.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, vigente con última reforma publicada el 14 de noviembre de 2025.
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, publicada y vigente conforme al Periódico Oficial número 113 de fecha 17 de junio de 2026.
- Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y demás disposiciones estatales aplicables.
- Normatividad archivística aplicable a la conservación, transferencia, baja y disposición documental.
- Reglamentos, lineamientos, políticas internas, manuales de organización y procedimientos de COAPAM que resulten aplicables.

Nota jurídica: La legislación estatal de 2026 define el Documento de Seguridad como el instrumento que describe las medidas técnicas, físicas y administrativas adoptadas para garantizar confidencialidad, integridad y disponibilidad; asimismo, exige inventario, funciones y obligaciones, análisis de riesgos y brecha, plan de trabajo, monitoreo y capacitación. Los artículos 25 a 36 regulan medidas de seguridad y vulneraciones, y los artículos 77 y 78 establecen atribuciones del Comité de Transparencia.

4. DEFINICIONES

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

6. ESTRUCTURA DE RESPONSABILIDADES

La protección de datos personales es una responsabilidad institucional y transversal. Cada área deberá identificar a las personas que participan en los tratamientos y documentar sus funciones.

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

7. INVENTARIO DE DATOS PERSONALES Y SISTEMAS DE TRATAMIENTO

El inventario deberá mantenerse actualizado. Cada tratamiento deberá contar, como mínimo, con: nombre del tratamiento; área responsable; finalidad; personas titulares; categorías de datos; medios de obtención; soporte; ubicación; personas con acceso; transferencias o remisiones; plazo de conservación; nivel de riesgo; medidas de seguridad y responsable operativo.

Área	Tratamiento / sistema	Datos personales probables	Soporte	Nivel inicial a validar
Comercial	Contratos, Padrón y expediente de usuarios	Nombre, domicilio, teléfono, correo, datos de contrato/cuenta, historial de pagos y adeudos	Digital y físico	Medio/Alto
Operativa	Órdenes de trabajo y atención de servicios	Nombre, domicilio, contacto, ubicación del servicio, fotografías cuando proceda	Físico	Medio
Administrativa	Facturación y pagos	Identificación, datos de contacto y datos relacionados con pagos/facturación	Digital	Medio/Alto
Administrativa	Expedientes de personal	Identificación, contacto, documentación laboral, bancaria y fiscal; otros	Digital y físico	Alto

		datos que sean estrictamente necesarios		
Administrativa	Proveedores y contratistas	Identificación, contacto, datos fiscales y bancarios de personas físicas, cuando corresponda	Digital y físico	Medio/Alto
Cultura del Agua	Participantes y actividades	Nombre, institución, grado/grupo, contacto; imágenes cuando se recaben	Digital y físico	Medio
Transparencia	Derechos ARCO y solicitudes	Datos identificativos y datos contenidos en las solicitudes y expedientes	Digital y físico	Alto

Los datos anteriores son una guía inicial y no sustituyen el levantamiento institucional. Cada coordinación deberá validar qué datos efectivamente trata, con qué finalidad, bajo qué fundamento, quién tiene acceso y cuánto tiempo deben conservarse.

8. IDENTIFICACIÓN DE TRATAMIENTOS POR ÁREA

Unidad de Transparencia

- Recepción, registro y seguimiento de solicitudes de derechos ARCO.
- Integración de expedientes para acreditar identidad y representación cuando proceda.



- Coordinación con las áreas que poseen los datos para localizar y entregar información.
- Elaboración y actualización de avisos de privacidad y documentación institucional.
- Registro y seguimiento de vulneraciones de seguridad.
- Control de solicitudes, plazos y comunicaciones relacionadas con protección de datos.

Coordinación Operativa

- Atención de reportes y órdenes de trabajo.
- Inspecciones, verificaciones y visitas a domicilios o instalaciones.
- Uso de fotografías o evidencias de campo cuando permitan identificar personas.
- Comunicación de información a otras áreas exclusivamente cuando sea necesaria para una función institucional.

Coordinación Comercial

- Alta, modificación y baja de cuentas de usuarios.
- Contratación y actualización de datos del servicio.
- Pagos, convenios, descuentos y aclaraciones.
- Atención de solicitudes de usuarios y seguimiento de adeudos.
- Consulta e intercambio de información con otras áreas para prestar el servicio.

Coordinación Administrativa

- Integración y resguardo de expedientes de personal.
- Procesamiento de nómina y prestaciones.
- Contratación y gestión de proveedores y prestadores de servicios.
- Comprobación de gastos, viáticos y pagos.
- Control de asistencia y documentación administrativa.



Coordinación de Cultura del Agua

- Registro de participantes menores de edad en actividades.
- Constancias.
- Gestión de datos de contacto para actividades institucionales.
- Obtención y uso de fotografías o videos de actividades, observando el aviso de privacidad y las reglas aplicables.
- Intercambio de información con CEAS Y CONAGUA.

9. CLASIFICACIÓN Y NIVEL DE RIESGO

El nivel de riesgo deberá determinarse considerando, entre otros elementos, la sensibilidad de los datos, el volumen de titulares, las transferencias, las vulnerabilidades existentes, las consecuencias para las personas titulares, el desarrollo tecnológico y antecedentes de incidentes.

Nivel	Criterios orientativos	Ejemplos
Bajo	Pocos titulares, datos de contacto básicos, acceso limitado y consecuencias acotadas.	Registros generales de actividades públicas sin datos sensibles.
Medio	Volumen relevante, datos identificativos o patrimoniales, múltiples usuarios o accesos.	Padrón de usuarios, órdenes de trabajo, registros de participantes.
Alto	Datos que pueden generar afectaciones importantes, expedientes laborales, información patrimonial extensa o sistemas críticos.	Expedientes de personal, derechos ARCO, bases con gran volumen de información vinculable a personas.

10. MEDIDAS DE SEGURIDAD ADMINISTRATIVAS

- Contar con políticas internas de protección de datos y confidencialidad.
- Asignar funciones y privilegios conforme al principio de necesidad de conocer.
- Mantener inventario de tratamientos y sistemas.
- Aplicar avisos de privacidad en los puntos de obtención de datos.
- Evitar la recopilación de datos que no sean necesarios para la finalidad.
- Establecer procedimientos de alta, cambio y baja de accesos.
- Formalizar obligaciones de confidencialidad para el personal y terceros cuando corresponda.
- Definir plazos de conservación conforme a la normatividad archivística y administrativa.
- Establecer procedimientos de supresión o destrucción segura cuando proceda.
- Registrar y atender vulneraciones de seguridad.
- Realizar análisis de riesgos y brechas al menos anualmente y cuando haya cambios relevantes.
- Capacitar al personal según su rol.
- Revisar periódicamente las medidas y documentar resultados.

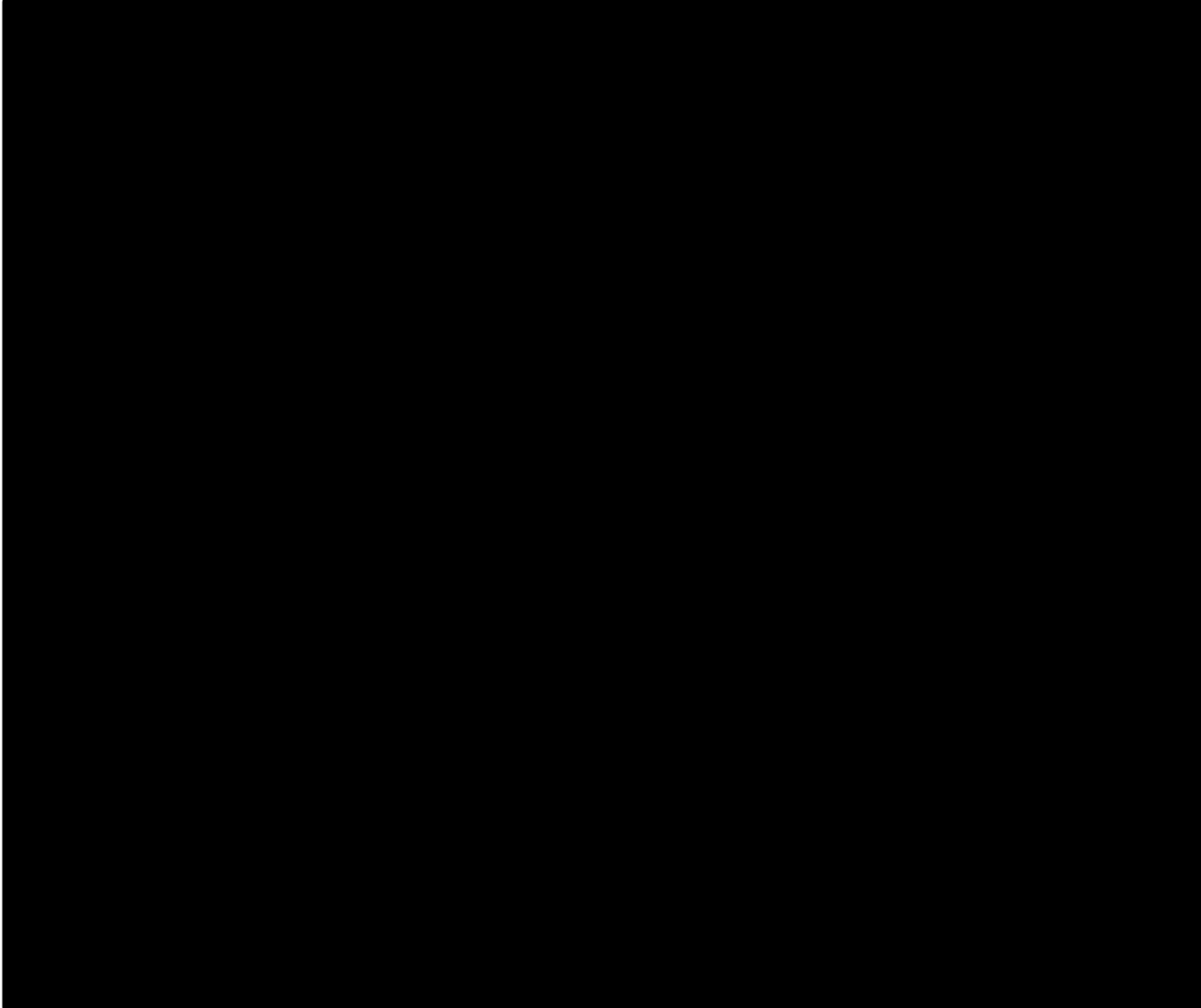
11. MEDIDAS DE SEGURIDAD FÍSICAS

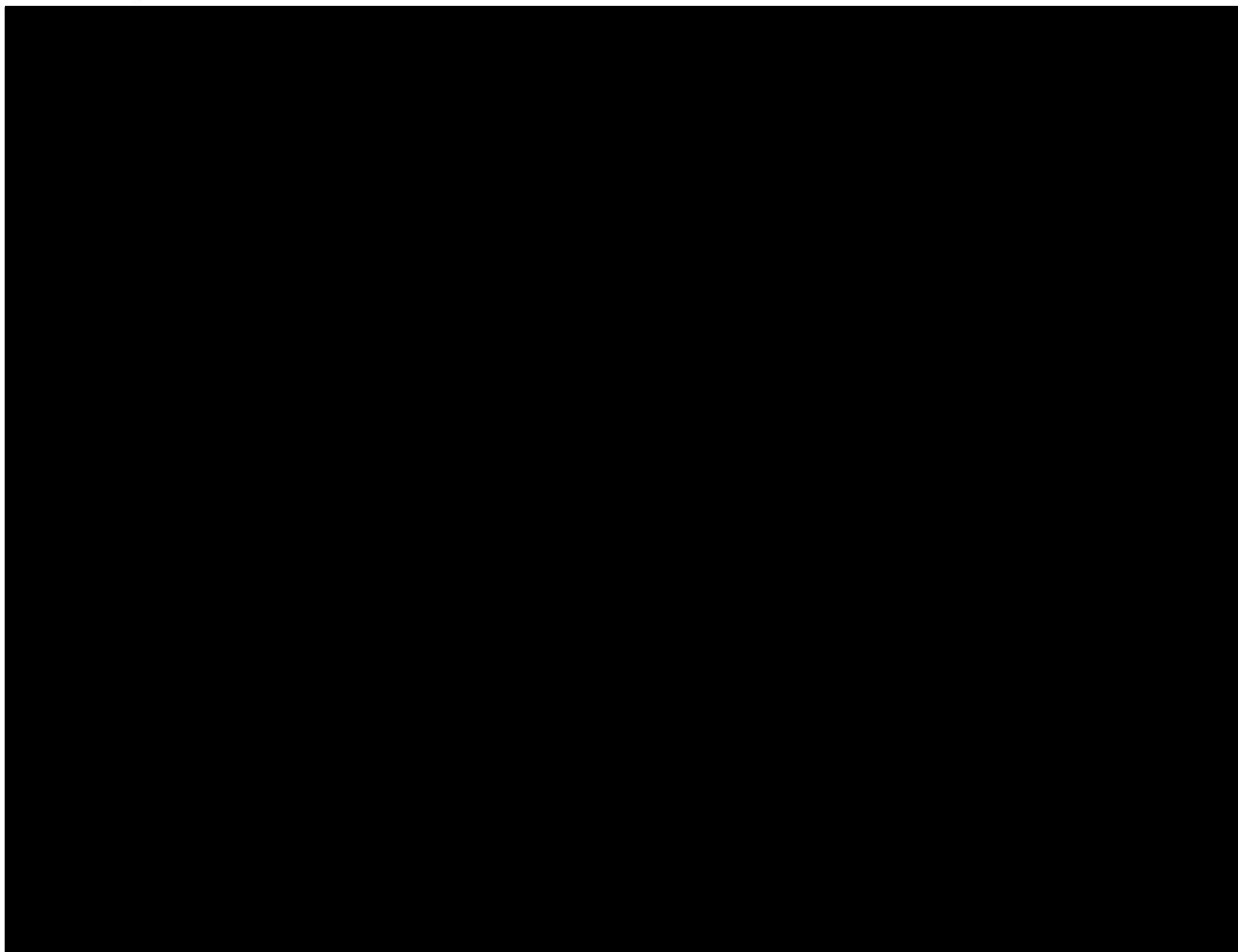
- Restringir el acceso a archivos y áreas donde se resguarden datos personales.
- Mantener expedientes físicos en archiveros, gavetas o espacios cerrados cuando no estén en uso.
- No dejar expedientes, listas, recibos o documentos con datos personales sobre escritorios de manera innecesaria.
- Controlar el préstamo y devolución de expedientes físicos.
- Proteger equipos portátiles y soportes removibles contra extravío.
- Evitar que visitantes o personal no autorizado observen pantallas o documentos.
- Disponer de mecanismos de prevención de incendios, humedad, inundación y otros riesgos físicos conforme a las condiciones del inmueble.
- Realizar mantenimiento preventivo de equipos y espacios de archivo.
- Aplicar destrucción segura de documentos físicos mediante procedimientos autorizados y compatibles con las obligaciones de archivo.

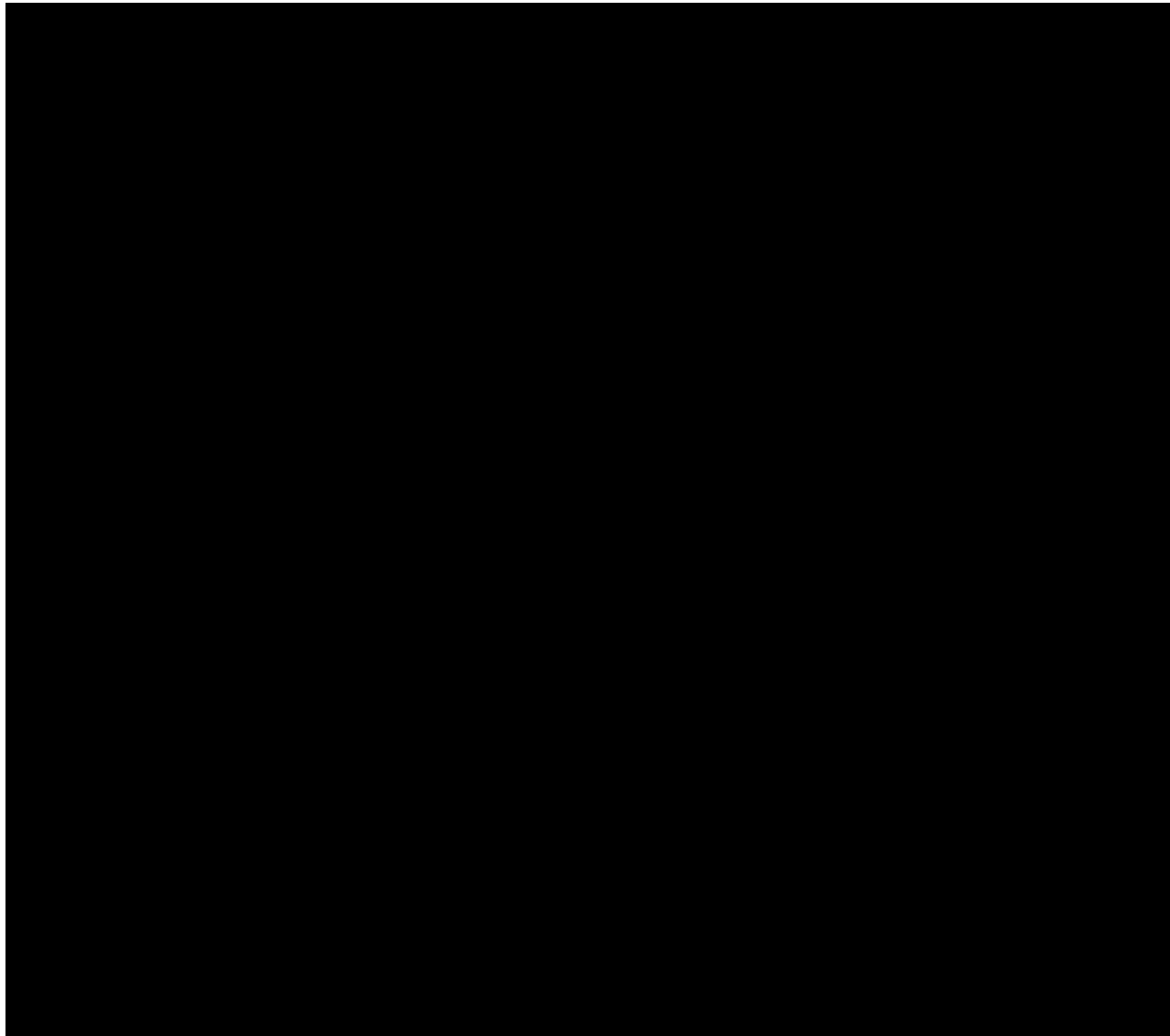
12. MEDIDAS DE SEGURIDAD TÉCNICAS

- Utilizar cuentas individuales; evitar compartir contraseñas.
- Aplicar contraseñas robustas y, cuando sea técnicamente posible, autenticación multifactor en sistemas que manejen información de mayor riesgo.
- Asignar privilegios conforme a las funciones del puesto.
- Bloquear sesiones cuando el equipo quede desatendido.
- Mantener sistemas operativos, aplicaciones y soluciones de seguridad actualizados.
- Contar con antivirus y protección de dispositivos cuando resulte aplicable.
- Realizar respaldos periódicos y verificar su recuperación.
- Restringir el uso de memorias USB y otros medios removibles cuando exista una alternativa institucional.
- Proteger la transmisión de datos mediante mecanismos de seguridad disponibles y adecuados.
- Registrar accesos o actividades críticas cuando los sistemas lo permitan.
- Eliminar de forma segura archivos o dispositivos cuando ya no deban conservarse y exista autorización para ello.
- Proteger equipos portátiles utilizados fuera de las instalaciones.
- No enviar bases de datos completas por correo o mensajería instantánea cuando existan medios institucionales más seguros.

13. ANÁLISIS DE RIESGOS







16. GESTIÓN DE VULNERACIONES DE SEGURIDAD

Ante cualquier pérdida, robo, extravío, copia, acceso, uso, tratamiento, daño, alteración o modificación no autorizada de datos personales, la persona que tenga conocimiento deberá reportarlo inmediatamente al superior jerárquico y a la Unidad de Transparencia o área institucional designada para coordinar la atención.

1. Detectar y reportar el incidente de inmediato.
2. Preservar evidencia disponible sin alterar innecesariamente los sistemas o documentos.
3. Contener el incidente: retirar accesos, aislar equipos o recuperar documentos, según corresponda.
4. Identificar los datos, personas titulares, sistemas y áreas afectadas.
5. Evaluar el impacto y las consecuencias.
6. Documentar el incidente en la bitácora de vulneraciones.
7. Implementar medidas correctivas inmediatas.
8. Determinar si corresponde informar a las personas titulares y a la autoridad competente, conforme a la legislación.
9. Realizar análisis de causa raíz.
10. Integrar acciones preventivas y correctivas al plan de trabajo.
11. Dar seguimiento hasta el cierre documentado.

La comunicación a las personas titulares, cuando legalmente proceda, deberá incluir al menos la naturaleza del incidente, los datos comprometidos, recomendaciones, acciones correctivas y medios para obtener información.

17. RESPALDO, RECUPERACIÓN Y CONTINUIDAD

- Identificar sistemas y archivos críticos.
- Definir periodicidad de respaldo según el nivel de riesgo.
- Conservar respaldos en una ubicación separada del equipo o sistema principal cuando sea posible.
- Restringir el acceso a respaldos.
- Probar periódicamente la recuperación de información.
- Documentar resultados de las pruebas.

- Contar con procedimientos para continuidad ante fallas de energía, equipos, red, software, inundación, incendio u otros eventos relevantes.
- Priorizar la recuperación de sistemas esenciales para la prestación del servicio y la atención a personas usuarias.

18. GESTIÓN DE TERCEROS Y PERSONAS ENCARGADAS

- Identificar a terceros que tengan acceso o traten datos personales por cuenta de COAPAM.
- Formalizar contractualmente las obligaciones de confidencialidad, seguridad, finalidad y tratamiento limitado.
- Definir mecanismos para comunicar y atender vulneraciones.
- Limitar el acceso de terceros a los datos estrictamente necesarios.
- Verificar que existan medidas de seguridad adecuadas al tratamiento.
- Al terminar la relación, recuperar o suprimir los datos conforme a las obligaciones legales y contractuales, salvo conservación obligatoria.

19. CAPACITACIÓN Y CONCIENTIZACIÓN

El programa general de capacitación deberá considerar, como mínimo:

Tema	Personal objetivo	Periodicidad sugerida	Evidencia
Principios y deberes de protección de datos	Todo el personal	Anual	Constancia
Derechos ARCO y atención de solicitudes	Transparencia y enlaces de áreas	Anual	Constancia
Seguridad de información y contraseñas	Todo el personal	Semestral	Constancia
Prevención y reporte	Todo el personal	Anual	Constancia

de incidentes			
Manejo seguro de expedientes físicos	Administrativa, Comercial, Operativa	Anual	Constancia
Uso de imágenes y actividades de Cultura del Agua	Cultura del Agua y personal relacionado	Anual	Constancia

20. MONITOREO, REVISIÓN Y ACTUALIZACIÓN

- Revisar semestralmente los controles de acceso a sistemas que contengan datos personales.
- Revisar anualmente el inventario de tratamientos.
- Evaluar anualmente el análisis de riesgos y brechas.
- Actualizar el Documento de Seguridad cuando cambien sustancialmente los tratamientos o el nivel de riesgo.
- Actualizarlo como resultado de incidentes y de acciones correctivas o preventivas.
- Documentar hallazgos, responsables, fechas compromiso y evidencia de cierre.
- Presentar al Comité de Transparencia los resultados relevantes para su seguimiento.

21. CONTROL DOCUMENTAL

Versión	Fecha	Descripción	Elaboró	Revisó	Aprobó
1.0	Septiembre 2026	Emisión inicial	Unidad de Transparencia	Lic. Verónica Nazaret Alfonzo Guizar	Comité de Transparencia

22. APROBACIÓN

El presente Documento de Seguridad deberá ser sometido a revisión jurídica y administrativa, validación por las áreas responsables y, en su caso, aprobación por el Comité de Transparencia de COAPAM, de conformidad con las disposiciones aplicables.

Cargo	Nombre	Firma
Titular de COAPAM	C.P José Alfredo Jimenéz García	
Titular de la Unidad de Transparencia	Lic. Verónica Nazaret Alfonzo Guizar	
Coordinación Operativa	Ing. Ramiro Borja Domínguez	
Coordinación Comercial	Lic. Pedro Luis López Morales	
Coordinación Administrativa	Lic. Lucia Guadalupe Guzman Guillén.	
Coordinación de Cultura del Agua	C.P José Alfredo Jimenéz García	
Presidencia/Integrantes del Comité de Transparencia	Lic. Mario Villatoro Vazquez (Presidente) C.P Rafael Humberto López Gómez (Secretario) Lic. Verónica Nazaret Alfonzo Guizar (Vocal)	

ANEXO 1. FUENTES NORMATIVAS OFICIALES CONSULTADAS

1. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, texto vigente publicado por el H. Congreso del Estado de Chiapas, con reforma publicada el 17 de junio de 2026.
2. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, texto vigente publicado por la Cámara de Diputados.
3. Legislación vigente del H. Congreso del Estado de Chiapas en materia de protección de datos personales y transparencia.

Referencias oficiales consultadas para la elaboración: Congreso del Estado de Chiapas y Cámara de Diputados del H. Congreso de la Unión.

NOTA FINAL DE IMPLEMENTACIÓN

Este documento constituye una base institucional integral para COAPAM. Antes de su aprobación definitiva deberá realizarse el levantamiento real de inventarios, sistemas, responsables, ubicaciones, transferencias, plazos de conservación, controles tecnológicos y evidencias existentes. Los campos marcados para validar deberán ser completados por las áreas correspondientes. La Unidad de Transparencia deberá coordinar la integración de la versión final y someterla a las instancias competentes.