



DOCUMENTO DE SEGURIDAD

SAPAM

**Sistema de Agua Potable y Alcantarillado Municipal
Pichucalco, Chiapas
2024 - 2027**





ÍNDICE	
PRESENTACION	3
OBJETIVOS DEL DOCUMENTO DE SEGURIDAD	4
RESPONSABILIDADES	4
ALCANCE DEL DOCUMENTO DE SEGURIDAD	5
SISTEMA DE GESTIÓN DE LOS DATOS PERSONALES	6
INVENTARIO DE TRATAMIENTOS Y DATOS PERSONALES	7
FUNCIONES Y RESPONSABILIDADES DEL TRATAMIENTO DE DATOS PERSONALES	9
PROGRAMA DE TRABAJO PARA LA IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD	13
ANÁLISIS DE RIESGO Y BRECHA	14
ANÁLISIS DE LA INFORMACIÓN	16
MEDIDAS DE SEGURIDAD	16
MONITOREO DE MEDIDAS DE SEGURIDAD	17
PROPUESTA DE CAPACITACIÓN EN MATERIA DE DATOS PERSONALES	17





PRESENTACION

La protección de datos personales forma parte de la prestación responsable de los servicios públicos. En SAPAM, la información relacionada con contratos, domicilios de servicio, consumos, pagos, reportes y trámites administrativos debe manejarse de manera ordenada, limitada a fines legítimos y con controles que reduzcan la posibilidad de que sea consultada o utilizada por personas no autorizadas.

Este documento constituye una guía institucional de trabajo. Su aplicación requiere que la Dirección de SAPAM y las personas responsables de cada proceso verifiquen las prácticas reales, completen los datos pendientes y documenten los controles que efectivamente existan. Las actividades descritas como propuestas no deben considerarse implementadas hasta que exista evidencia de su ejecución.

El Sistema de Agua Potable y Alcantarillado Municipal de Pichucalco, Chiapas (SAPAM), en el ejercicio de sus atribuciones y funciones, realiza operaciones que pueden involucrar la obtención, uso, registro, organización, conservación, consulta y, en su caso, transferencia de datos personales de usuarios, solicitantes, proveedores y personas servidoras públicas.

El presente Documento de Seguridad establece un marco de referencia para identificar y proteger los datos personales tratados por SAPAM, mediante medidas administrativas, físicas y técnicas orientadas a preservar su confidencialidad, integridad y disponibilidad, prevenir accesos no autorizados y reducir los riesgos de pérdida, alteración, daño o divulgación indebida.





OBJETIVOS DEL DOCUMENTO DE SEGURIDAD

Establecer criterios y acciones para proteger los datos personales que SAPAM trate en el cumplimiento de sus funciones.

- Identificar los procesos y las categorías de datos personales tratados por SAPAM.
- Definir responsabilidades para las personas que acceden a datos personales.
- Prevenir, detectar y atender riesgos relacionados con el acceso, uso, pérdida, alteración o divulgación no autorizados.
- Establecer medidas administrativas, físicas y técnicas proporcionales al tipo de información y a los riesgos identificados.
- Mantener actualizado el inventario de tratamientos y promover la capacitación del personal.

La implementación deberá realizarse conforme a la normativa aplicable en materia de protección de datos personales y transparencia para los sujetos obligados del Estado de Chiapas

Objetivos específicos y resultados esperados

- Contar con una relación documentada de los tratamientos de datos personales que efectivamente realiza SAPAM y de las personas responsables de cada uno.
- Asegurar que la información se recabe para una finalidad determinada y que el personal conozca qué datos puede consultar, modificar, imprimir o entregar.
- Reducir los riesgos de pérdida, extravío, consulta indebida, alteración, envío equivocado o divulgación de documentos y archivos electrónicos.
- Establecer una ruta de actuación ante incidentes, con registro, comunicación interna, análisis de causas y medidas correctivas.
- Definir un programa de revisión y capacitación que permita mejorar los controles y actualizar el documento cuando cambien los procesos.

RESPONSABILIDADES

La dirección de SAPAM deberá impulsar la implementación de este documento, sin sustituir las atribuciones que legalmente correspondan al Comité de Transparencia, a la Unidad de Transparencia, al oficial o enlace de protección de datos personales, cuando exista, ni a las áreas administrativas competentes.

- Dirección de SAPAM: promover el cumplimiento del documento, asignar responsables y facilitar los recursos necesarios.
- Responsables de procesos: identificar los datos que recaban, documentar las finalidades, limitar el acceso y reportar incidentes.
- Personal usuario de información: utilizar los datos únicamente para funciones autorizadas, mantener la confidencialidad y proteger expedientes, equipos y credenciales.



- Área o personal de tecnologías de la información, si corresponde: apoyar en controles de acceso, respaldos, actualizaciones y atención de incidentes.
- Unidad de Transparencia y Comité de Transparencia, según sus atribuciones: orientar y coordinar el cumplimiento normativo, la atención de derechos ARCO y la revisión de medidas.

Reglas generales de responsabilidad

- Cada persona servidora pública debe utilizar la información únicamente para las tareas que le hayan sido asignadas y evitar consultas por curiosidad o por motivos personales.
- No se deberán entregar padrones, listados, recibos, domicilios, teléfonos, expedientes ni capturas de pantalla a terceros sin autorización y sin verificar el fundamento y la finalidad de la entrega.
- Los documentos impresos deberán retirarse oportunamente de impresoras, escritorios, vehículos y áreas de atención; al terminar la jornada, deberán guardarse en el lugar autorizado.
- Las contraseñas son personales e intransferibles. Cuando una persona requiera acceso a un sistema, deberá solicitar su propia cuenta o el permiso correspondiente.

Cualquier pérdida de documentos, dispositivo, archivo, envío equivocado o acceso inusual deberá reportarse de inmediato a la jefatura o persona designada, sin intentar ocultar el incidente.

ALCANCE DEL DOCUMENTO DE SEGURIDAD

El documento aplica exclusivamente a los procesos y al personal de SAPAM que trate datos personales, tanto en expedientes físicos como en archivos electrónicos, sistemas informáticos, equipos de cómputo, correo institucional y demás medios autorizados.

De manera preliminar, el alcance puede comprender los procesos de alta y actualización de usuarios del servicio; contratación o convenios; facturación y cobranza; registro de pagos; lectura y control de medidores; atención de reportes, quejas y solicitudes; trámites administrativos; gestión de proveedores y personal. SAPAM deberá confirmar cuáles de estos procesos realiza efectivamente y agregar o retirar los que correspondan.

Medios comprendidos

El alcance comprende la información que se encuentre en formatos de contratación, solicitudes, contratos de servicio, recibos, comprobantes, órdenes de trabajo, reportes de fugas o fallas, listados de usuarios, expedientes de proveedores y personal, correos institucionales, hojas de cálculo, archivos compartidos y sistemas utilizados para la operación. La inclusión de un medio en esta lista deberá confirmarse con SAPAM y ajustarse a los recursos que realmente utiliza.



Ciclo de vida de los datos personales

1. Obtención: recabar únicamente los datos necesarios para el trámite o servicio e informar al titular mediante el aviso de privacidad aplicable.
2. Registro y organización: capturar la información de forma legible y correcta, evitar duplicidades innecesarias y utilizar formatos autorizados.
3. Uso y consulta: permitir el acceso solo al personal que lo necesita para cumplir sus funciones.
4. Comunicación o transferencia: comprobar la identidad del destinatario, la finalidad, la autorización y el fundamento jurídico antes de compartir información.
5. Conservación: mantener expedientes físicos y electrónicos en lugares y sistemas autorizados, durante los plazos aplicables.
6. Bloqueo, supresión o destrucción: aplicar las reglas de archivo y conservación que correspondan, evitando eliminar documentos antes de tiempo o conservarlos indefinidamente sin justificación.

Revisión documental

El inventario, los avisos de privacidad, las listas de acceso, los procedimientos y el propio Documento de Seguridad deberán revisarse cuando se incorpore un nuevo sistema, cambie un formato, se modifique la finalidad de un trámite, se detecte un incidente o cambie la estructura organizacional.

SISTEMA DE GESTIÓN DE LOS DATOS PERSONALES

El sistema de gestión de datos personales de SAPAM comprende las políticas, procedimientos, controles y registros que permitan administrar el ciclo de vida de los datos, desde su obtención hasta su conservación, bloqueo, supresión o destrucción conforme a las disposiciones aplicables.

Para operarlo, SAPAM deberá: a) identificar los procesos y sus finalidades; b) mantener un inventario actualizado; c) establecer perfiles y permisos de acceso; d) resguardar documentos y equipos; e) documentar las transferencias; f) atender solicitudes de derechos ARCO mediante los canales institucionales correspondientes; g) revisar periódicamente los controles; y h) capacitar al personal.

Los datos deberán recabarse por medios lícitos, ser pertinentes y limitarse a lo necesario para la finalidad informada. El personal no deberá compartir contraseñas, utilizar bases de datos para fines ajenos a sus funciones ni conservar información más tiempo del permitido por las reglas archivísticas y disposiciones aplicables.



INVENTARIO DE TRATAMIENTOS Y DATOS PERSONALES

El siguiente inventario es una propuesta inicial basada en funciones típicas de un organismo operador de agua potable y alcantarillado. No constituye una certificación de que todos los tratamientos se encuentren actualmente implementados en SAPAM. El área deberá validar, completar o eliminar cada registro antes de aprobar la versión definitiva.

Proceso propuesto	Titulares datos que podrían tratarse	Finalidad	Medio soporte	Validación requerida
Registro y de padrón de usuarios	Nombre, domicilio del servicio, teléfono, correo, identificación y datos del predio cuando proceda	Identificar al usuario y administrar el servicio	Expediente físico y/o sistema	Confirmar campos, sistema y responsable
Contratación y convenios	Identificación, domicilio, firma, datos de contacto y documentos presentados	Formalizar alta, cambio o convenio del servicio	Formato, expediente y/o sistema	Confirmar documentos y fundamento
Facturación y cobranza	Nombre, cuenta o contrato, domicilio, consumos, saldos y pagos	Emitir recibos y administrar adeudos	Sistema comercial, recibos y archivos	Confirmar sistemas y accesos
Registro de pagos	Referencia de contrato, importe, fecha y comprobante; datos bancarios solo si se reciben	Registrar y conciliar pagos	Sistema, caja y comprobantes	Confirmar medios de pago y datos capturados
Lectura y control de medidores	Cuenta de usuario, domicilio, lectura y consumo	Calcular consumos y dar seguimiento al servicio	Formatos, dispositivos o sistema	Confirmar si hay aplicación/dispositivo



Reportes, quejas y solicitudes	Nombre, contacto, domicilio, número de contrato y descripción del reporte	Atender incidencias y dar seguimiento	Ventanilla, teléfono, correo o sistema	Confirmar canales y plazos
Gestión de proveedores	Nombre de contacto, teléfono, correo, firma y datos fiscales cuando correspondan	Administrar compras, servicios y pagos	Expediente físico y/o electrónico	Confirmar si SAPAM conserva estos expedientes
Administración de personal	Identificación, contacto, datos laborales y, cuando corresponda, nómina y datos patrimoniales	Gestionar la relación laboral y obligaciones aplicables	Expediente laboral y sistema autorizado	Confirmar qué datos conserva SAPAM y quién los custodia

Categorías preliminares: datos de identificación y contacto; datos relacionados con la prestación del servicio; datos patrimoniales o financieros únicamente cuando se recaben; y datos laborales respecto del personal. No se presume que SAPAM trate datos personales sensibles. Si algún proceso los requiere, deberá identificarse expresamente, justificar su necesidad y aplicar controles reforzados.

Para cada tratamiento validado se deberá registrar, como mínimo: nombre del proceso; finalidad; fundamento; categorías y tipos de datos; origen y medio de obtención; ubicación de expedientes o bases; personas con acceso; plazo de conservación; transferencias y destinatarios; medidas de seguridad; y nombre y cargo del responsable.

Criterios para completar el inventario

- Registrar el nombre exacto del trámite o proceso y describirlo de manera comprensible.
- Indicar de dónde provienen los datos: directamente de la persona titular, de su representante o de otra fuente legalmente permitida.
- Precisar las categorías de datos recabados, evitando incluir campos que no sean necesarios para el propósito del trámite.
- Identificar el soporte y ubicación institucional: expediente físico, sistema, equipo autorizado, correo institucional o archivo compartido.
- Señalar qué puestos tienen acceso y por qué lo requieren, incluyendo permisos para consultar, modificar, exportar o imprimir.



- Documentar si existe transferencia a otra autoridad o tercero, quién recibe los datos, con qué finalidad y cuál es el fundamento que la permite.
- Indicar el plazo de conservación conforme al catálogo de disposición documental y demás reglas aplicables, sin establecer plazos arbitrarios.
- Actualizar el registro cuando se agreguen campos, se cambien los sistemas, se suspenda un proceso o cambie el personal responsable.

Registros complementarios sugeridos

Registro	Contenido mínimo	Responsable sugerido
Relación de sistemas y archivos	Nombre del sistema o archivo, finalidad, ubicación institucional, responsable y personas con acceso	Responsable del proceso y apoyo técnico
Control de usuarios y permisos	Cuenta asignada, puesto, permisos, fecha de alta, modificación o baja	Responsable del sistema o Dirección
Control de préstamo de expedientes	Expediente, persona que lo solicita, motivo, fecha de salida y devolución	Custodio del archivo
Registro de incidentes	Fecha, tipo de incidente, datos potencialmente afectados, acciones inmediatas, seguimiento y cierre	Persona designada por SAPAM
Registro de transferencias	Destinatario, finalidad, datos enviados, fundamento, medio de envío y evidencia	Responsable del proceso

FUNCIONES Y RESPONSABILIDADES DEL TRATAMIENTO DE DATOS PERSONALES

La asignación definitiva de responsables deberá realizarse mediante nombres y cargos confirmados por SAPAM. La siguiente matriz funcional es orientativa y debe adecuarse al organigrama vigente.

Función o proceso	Responsabilidad principal	Acciones de control
Dirección de SAPAM	Supervisión general	Designar responsables, aprobar procedimientos y revisar incidencias



Atención a usuarios / padrón	Registro y actualización de usuarios	Verificar identidad cuando proceda, limitar captura y resguardar expedientes
Caja / facturación / cobranza	Registro de recibos y pagos	Conciliar registros, controlar acceso y evitar exposición de recibos o reportes
Operación / lectura de medidores	Registro de lecturas e incidencias del servicio	Usar solo datos necesarios y entregar información por canales autorizados
Administración / recursos humanos, si corresponde	Expedientes del personal y proveedores	Separar expedientes, restringir accesos y cumplir plazos de conservación
Tecnologías de información, si corresponde	Soporte a sistemas y equipos	Administrar cuentas, respaldos, actualizaciones y bitácoras
Todo el personal autorizado	Uso adecuado de los datos	Confidencialidad, escritorio limpio, bloqueo de sesión y reporte inmediato de incidentes

El acceso deberá otorgarse bajo el principio de necesidad de conocer y de acuerdo con las funciones de cada puesto. Los cambios de puesto, bajas o terminación de funciones deberán reflejarse oportunamente en los permisos de acceso.

Estructura de puestos de SAPAM y responsabilidades relacionadas con el manejo de información

Con base en el organigrama proporcionado, se incorporan únicamente las denominaciones de los cargos, sin nombres propios. Las responsabilidades siguientes son generales y deberán ajustarse a las funciones formalmente asignadas a cada puesto.

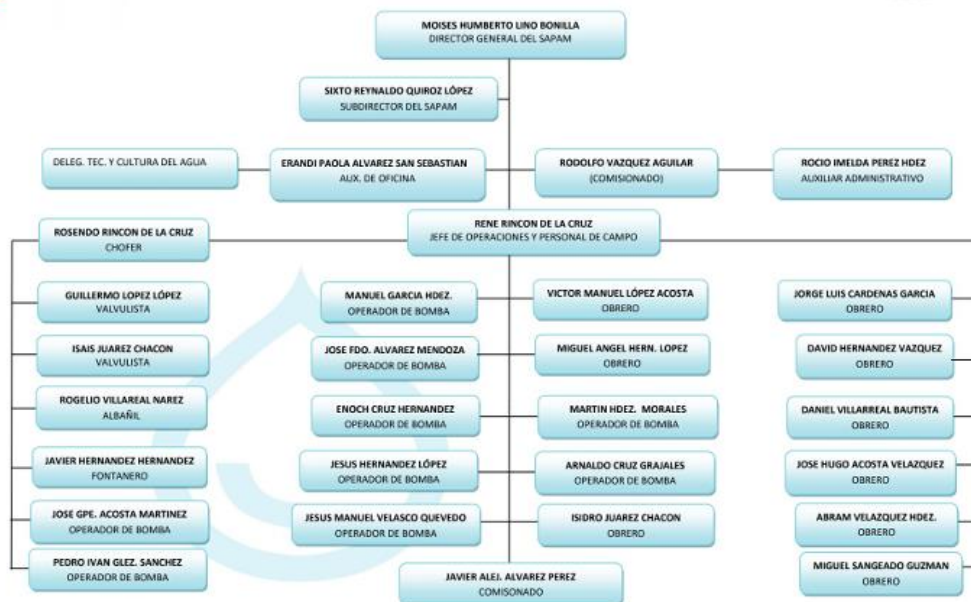
Cargo	Responsabilidad general relacionada con datos personales
Director General del SAPAM	Supervisar el cumplimiento de las medidas de protección de datos personales y promover los recursos necesarios.
Subdirector del SAPAM	Apoyar la coordinación y seguimiento de los procedimientos internos de resguardo de información.
Delegación Técnica y Cultura del Agua	Resguardar los datos que se reciban o generen en actividades técnicas,



	educativas y de cultura del agua, cuando corresponda.
Auxiliar de oficina	Apoyar la recepción, organización, archivo y canalización de documentos, evitando accesos o divulgaciones no autorizadas.
Comisionado	Tratar únicamente la información necesaria para las funciones formalmente encomendadas y mantener su confidencialidad.
Auxiliar administrativo	Capturar, consultar y organizar información administrativa solo para fines autorizados y con acceso limitado.
Jefe de Operaciones y Personal de Campo	Coordinar el manejo de reportes operativos y la información necesaria para organizar al personal de campo.
Chofer	Proteger los documentos o datos que, en su caso, le sean confiados durante el desempeño de sus funciones.
Valvulista	Utilizar únicamente los datos operativos o de ubicación del servicio necesarios para las tareas asignadas.
Albañil	Resguardar la información de servicio que, en su caso, reciba para ejecutar trabajos autorizados.
Fontanero	Proteger los datos de reportes y domicilios de servicio a los que tenga acceso por motivo de sus labores.
Operador de bomba	Mantener la confidencialidad de los registros operativos o datos a los que tenga acceso.
Obrero	Usar y proteger la información que se le proporcione para realizar las actividades asignadas.



ESTRUCTURA ORGANIZACIONAL



GOBIERNO MUNICIPAL 2024-2027

Todo el personal, independientemente del cargo, deberá guardar confidencialidad, evitar compartir contraseñas, entregar información solo por canales autorizados y reportar de inmediato cualquier pérdida, envío equivocado o acceso no autorizado.

Criterios de actuación por puesto

Las funciones incluidas en la tabla de cargos deben entenderse como controles generales. No significan que cada puesto necesariamente trate todos los tipos de datos personales. El acceso se limita a la información indispensable para la tarea encomendada y debe revisarse cuando cambien las funciones.

- El personal operativo de campo deberá recibir únicamente los datos necesarios para atender una orden de trabajo o reporte. Cuando no requiera conocer datos identificativos completos, se deberá valorar el uso de folios o referencias de servicio.
- El personal administrativo deberá proteger los documentos y archivos que reciba, evitar copias innecesarias y verificar que los destinatarios estén autorizados antes de entregar información.
- Las jefaturas deberán comunicar cambios de adscripción, bajas y necesidades de acceso para que los permisos se actualicen oportunamente.

El personal que reciba solicitudes de información o de acceso a datos personales deberá canalizarlas a la instancia competente, sin resolverlas por cuenta propia cuando no tenga atribuciones.



PROGRAMA DE TRABAJO PARA LA IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD

El programa siguiente establece acciones mínimas propuestas. Las fechas y responsables deben asignarse al aprobar el documento.

Acción	Resultado esperado	Responsable sugerido	Periodicidad / plazo
Validar inventario de tratamientos	Inventario firmado y actualizado	Responsables de proceso y enlace de datos	Inicial y cada vez que cambien procesos
Revisar permisos de acceso	Listado vigente de usuarios y perfiles	Responsable de cada sistema / Dirección	Trimestral y ante cambios de personal
Ordenar y resguardar expedientes	Archivos identificados, bajo llave y con control de préstamo	Custodios de expedientes	Continuo; revisión trimestral
Establecer respaldo y recuperación	Copias de seguridad y prueba de restauración documentada	Responsable técnico, si existe	Según criticidad; prueba periódica
Documentar incidentes	Registro, atención y medidas correctivas	Dirección y enlace responsable	Cada incidente
Capacitar al personal	Lista de asistencia y materiales	Unidad de Transparencia / Dirección	Al ingreso y al menos anual
Revisar avisos de privacidad y formatos	Avisos vigentes y adecuados a cada trámite	Área competente	Inicial y ante cambios
Evaluar medidas y brechas	Plan de mejora con responsables y fechas	Dirección y responsables de proceso	Al menos anual

El programa debe conservar evidencia de ejecución: listas de verificación, actas, bitácoras, reportes de capacitación y registros de incidentes. Las acciones que no sean aplicables deberán justificarse por escrito.



SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD APARTADO DEL PROGRAMA DE TRABAJO PARA LA IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD.

Se testa el apartado que contiene el programa de trabajo para la implementación de medidas de seguridad, contiene información que identifica las vulnerabilidades 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 der la 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 en párrafo primero, de la ley de protección de datos personales en posesión de los 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.

ANÁLISIS DE RIESGO Y BRECHA

El análisis detallado de riesgos debe realizarse internamente con información actualizada sobre sistemas, ubicaciones, permisos y controles. Por seguridad, los detalles operativos que revelen vulnerabilidades, ubicaciones precisas, configuraciones o deficiencias específicas deberán manejarse como información de acceso restringido cuando así proceda conforme a la normativa aplicable.

Como categorías iniciales de amenaza se consideran: acceso no autorizado; pérdida o extravío de expedientes o dispositivos; divulgación accidental; alteración o destrucción de registros; malware o falla de equipo; uso de información para fines distintos; y envío de datos a destinatarios equivocados.

La evaluación deberá ponderar la probabilidad y el impacto para las personas titulares, el volumen y tipo de datos, el soporte utilizado, la cantidad de personas con acceso y la eficacia de las medidas existentes. No se asigna en este documento un nivel cuantitativo definitivo, pues requiere verificación de las condiciones reales de SAPAM.

La brecha se determinará comparando las medidas existentes con las necesarias. Para cada hallazgo deberán documentarse: riesgo, control existente, control faltante, nivel de prioridad, responsable, fecha compromiso y evidencia de cierre.



SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD, APARTADO DE ANÁLISIS DE RIESGO Y BRECHA.

Se testa el apartado que contiene el análisis de riesgo y brecha, contiene la información que identifica vulnerabilidades y 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 , dela ley de transparencia y acceso al a 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 los 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 las versiones públicas.

Metodología sugerida de valoración

Para cada proceso, SAPAM puede valorar la probabilidad de que ocurra un incidente y la gravedad de sus consecuencias para las personas titulares. La valoración debe considerar el tipo de datos, el número aproximado de titulares, la facilidad de acceso, el tiempo de exposición, la existencia de copias, la posibilidad de recuperación y los controles vigentes. La clasificación final deberá sustentarse en evidencia y no en estimaciones genéricas.

Nivel orientativo	Criterio de referencia	Respuesta sugerida
Bajo	La exposición es limitada, existen controles funcionales y la afectación potencial es reducida.	Mantener controles y revisar periódicamente.
Medio	Hay debilidades corregibles, acceso compartido o controles que requieren mayor seguimiento.	Asignar responsable y fecha de mejora; verificar el cierre.
Alto	Existe posibilidad relevante de acceso no autorizado, pérdida de información importante o afectación significativa a titulares.	Aplicar medidas inmediatas, restringir accesos y escalar a la Dirección y a la instancia competente.

La tabla anterior es una guía de trabajo y no sustituye una metodología formal aprobada. La evaluación concreta y sus detalles deberán conservarse bajo controles de acceso adecuados.



ANÁLISIS DE LA INFORMACIÓN

El análisis de la información deberá elaborarse a partir del inventario validado y de la evaluación de riesgos.

- Cuantificar los tratamientos efectivamente identificados en SAPAM.
- Determinar qué categorías de datos se utilizan en cada proceso.
- Identificar los soportes físicos y electrónicos y sus ubicaciones institucionales.
- Registrar qué procesos comparten información y cuál es la justificación de cada transferencia.
- Priorizar las medidas según la probabilidad e impacto de una vulneración.

Preguntas de verificación para el análisis

- ¿Se recaban únicamente los datos necesarios para el trámite?
- ¿Existe un aviso de privacidad disponible para las personas usuarias?
- ¿Los expedientes están organizados y se conoce quién los custodia?
- ¿Las cuentas y contraseñas son individuales y los permisos están actualizados?
- ¿Se realizan respaldos y se ha comprobado que pueden recuperarse?
- ¿Se conocen los canales autorizados para enviar información a otras áreas o autoridades?
- ¿El personal sabe a quién reportar un incidente y qué información debe proporcionar?
- ¿Existen reglas para conservar y eliminar documentos de acuerdo con los plazos aplicables?

MEDIDAS DE SEGURIDAD

Las medidas deberán ajustarse al tipo de datos, a las finalidades del tratamiento y al resultado del análisis de riesgo.

- Administrativas: políticas internas; designación de responsables; acuerdos o deberes de confidencialidad; control de préstamos; capacitación; gestión de incidentes; revisión de avisos de privacidad; y aplicación de plazos de conservación.
- Físicas: archiveros cerrados; control de llaves; acceso limitado a áreas de archivo; resguardo de equipos; destrucción segura de documentos; y prohibición de dejar expedientes a la vista.
- Técnicas: cuentas individuales; contraseñas robustas y no compartidas; bloqueo automático de sesión; permisos por función; actualizaciones; protección contra software malicioso; copias de seguridad; y eliminación segura de archivos cuando corresponda.
- Operativas: verificar destinatarios antes de enviar información; evitar el uso de cuentas personales o dispositivos no autorizados; no compartir listados completos si basta con información parcial; y reportar inmediatamente cualquier incidente.

La aplicación efectiva de cada medida deberá documentarse. Las medidas no implementadas deben incorporarse al programa de trabajo con responsable y fecha compromiso.



MONITOREO DE MEDIDAS DE SEGURIDAD

El monitoreo permitirá comprobar que los controles se mantengan vigentes y sean eficaces. Se recomienda realizar las siguientes actividades:

- Revisar periódicamente cuentas, permisos y contraseñas; revocar accesos que ya no sean necesarios.
- Verificar el cumplimiento de los procedimientos para consultar, imprimir, entregar y archivar información.
- Inspeccionar el resguardo de expedientes físicos y el control de llaves.
- Comprobar la ejecución de respaldos y documentar pruebas de recuperación.
- Registrar incidentes, causas, acciones correctivas y medidas para evitar recurrencias.
- Actualizar el inventario cuando se cree, modifique o elimine un proceso, formato o sistema.

Los resultados del monitoreo deberán asentarse en una bitácora o acta con fecha, responsable, hallazgos, acciones correctivas y fecha de seguimiento.

PROPUESTA DE CAPACITACIÓN EN MATERIA DE DATOS PERSONALES

SAPAM deberá promover la formación y sensibilización de las personas servidoras públicas que intervengan en el tratamiento de datos personales, con el fin de fortalecer el cumplimiento de la normativa y reducir errores operativos.

- Principios y deberes de protección de datos personales.
- Obligaciones de los sujetos obligados y responsabilidades del personal.
- Avisos de privacidad y finalidades del tratamiento.
- Identificación, clasificación y minimización de datos personales.
- Medidas de seguridad administrativas, físicas y técnicas.
- Atención de solicitudes de derechos ARCO y canalización a la Unidad de Transparencia.
- Gestión de incidentes, notificación interna y preservación de evidencia.
- Uso seguro de correo electrónico, sistemas, equipos y expedientes físicos.
- Conservación, archivo, bloqueo y destrucción segura de documentos.

La capacitación deberá programarse al ingreso del personal y actualizarse periódicamente. Se conservarán listas de asistencia, materiales, evaluaciones y constancias cuando existan.



Modalidad y evidencia de capacitación

La capacitación puede impartirse mediante sesiones presenciales, materiales de consulta o actividades internas de actualización. Debe adaptarse a las tareas del personal administrativo y operativo, utilizar ejemplos relacionados con los trámites y servicios de SAPAM, y dejar evidencia de fecha, tema, personas participantes y material entregado.

Tema	Personal prioritario	Evidencia sugerida
Principios, deberes y avisos de privacidad	Personal que recibe solicitudes o registra usuarios	Lista de asistencia y material
Resguardo físico de expedientes	Personal administrativo y custodios de archivo	Lista de verificación del área
Uso seguro de sistemas, correo y contraseñas	Personal con acceso a equipos y sistemas	Registro de capacitación
Manejo de reportes y órdenes de trabajo	Jefatura operativa y personal de campo	Instrucciones de trabajo y acuse
Atención y reporte de incidentes	Todo el personal	Protocolo difundido y simulación o ejercicio

