DOCUMENTO DE SEGURIDAD

Protección de Datos Personales

Sistema de Agua Potable, Alcantarillado y Saneamiento del municipio de San Julián (SAPAJ) 2021-2024

(347)718 19 27

LUCIANO HERNÁNDEZ No. 79 NTE.
sapaj@sanjulian.gob.mx
www.sanjulian.gob.mx
San Julián, Jal.

INDICE

SISTEMA DE AGUA POTABLE, ALCANTARILLADO Y SANEAMIENTO DEL MUNICIPIO DE SAN JULIAN (SAPAJ)

I. INTRODUCCIÓN

En el Sistema de Agua Potable, Alcantarillado y Saneamiento del municipio de San Julián (SAPAJ), la información es un activo que debe protegerse mediante un conjunto coherente de procesos y sistemas diseñados, administrados y mantenidos por la organización. De esta manera, la gestión de la seguridad de la información, como parte de un sistema administrativo más amplio, busca establecer, implementar, operar, monitorear y mejorar los procesos y sistemas relativos a la confidencialidad, integridad y disponibilidad de la información, aplicando un enfoque basado en los riesgos que la organización afronta.

El presente Documento de Seguridad para Sistemas de Datos Personales en medios físicos (Documento), se dicta en cumplimiento de las disposiciones jurídicas vigentes, para la mejor protección de los sistemas con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen.

El Documento brinda al SISTEMA DE AGUA POTABLE, ALCANTARILLADO Y SANEAMIENTO DEL MUNICIPIO DE SAN JULIAN (SAPAJ) homogeneidad en la organización, procesos y sistemas, en el que el Comité de Transparencia, conjuntamente con el área de Tecnologías de la Información y los responsables de los sistemas de datos personales, definen las medidas de seguridad administrativas, físicas y técnicas implementadas para la protección de los sistemas de datos personales custodiados.

II. GLOSARIO

II.1 Auditabilidad: Característica que permite la revisión y análisis de eventos y análisis para su control posterior.

II.2 Autenticidad: Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

II.3 Autentificar: Acción de comprobar que la persona es quien dice ser. Ello, mediante

el cotejo de uno o más datos en dicha identificación oficial contra (i) los datos en alguna otra identificación, documento, certificado digital (como el de la firma electrónica) o dispositivo que tenga la persona, (ii) los datos que sepa o tenga memorizados (su firma autógrafa o su contraseña, por ejemplo) o (iii) una o más características que coincidan con lo que es dicha persona (fotografía o huella dactilar, por ejemplo).

II.4 Autorizar: Se considera como el acceso que se le permite a la persona que se ha identificado y autenticado apropiadamente. Esto depende del o de los permisos que le conceda el responsable de autorizar los accesos.

II.5 Clasificación: Acto por el cual se determina que la información que posee el Sistema de Agua Potable, Alcantarillado y Saneamiento del municipio de San Julián (SAPAJ) es reservada o confidencial.

II.6 Confidencialidad: Propiedad de prevenir la divulgación de información a personas o sistemas no autorizados, y que garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma, es decir, asegurar que la misma no sea divulgada o accedida a personas o procesos no autorizados.

II.7 Datos personales: Cualquier información concerniente a una persona física identificada o de acceso a la información, a los datos personales y a la corrección de éstos, en unidades administrativas distintas al Sistema de Agua Potable, Alcantarillado y Saneamiento del municipio de San Julián (SAPAJ).

II.8 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 información y a los recursos relacionados con la misma, cada vez que lo requieran.

II.9 Documentos: Los expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, Instructivos, notas, memorandos, estadísticas o bien, cualquier otro registro que documente el ejercicio de las facultades o la actividad de los sujetos obligados y sus servidores públicos, sin importar su fuente o fecha de elaboración. Los documentos podrán estar en cualquier medio, sea escrito, impreso, sonoro, visual, electrónico, informático u holográfico.

II.10 Encargado: El servidor público o cualquier otra persona física o moral facultado por un instrumento jurídico o expresamente autorizado por el Responsable para llevar a cabo el tratamiento físico o automatizado de los datos personales.

II.11 Integridad: Es 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.

II.12 Lineamientos: Los actos administrativos de carácter general expedidos por el Pleno del Instituto y de observancia obligatoria.

II.12 Recursos públicos: Los recursos humanos, financieros y materiales con que cuenta el SISTEMA DE AGUA POTABLE, ALCANTARILLADO Y SANEAMIENTO DEL MUNICIPIO DE SAN JULIAN (SAPAJ), y que utiliza para alcanzar sus objetivos y producir los bienes o prestar los servicios que son de su competencia.

II.13 Responsable: El servidor público titular de la unidad administrativa designado por el titular de la dependencia o entidad, que decide sobre el tratamiento físico o automatizado de datos personales, así como el contenido y finalidad de los sistemas de datos personales.

II.14 Servidores públicos: Los mencionados en el párrafo primero del Artículo 108 Constitucional y todas aquellas personas que manejen o apliquen recursos públicos federales.

II.15 Sistema de datos personales: El conjunto ordenado de datos personales que estén en posesión de un sujeto obligado.

II.16 Titular de los datos: Persona física a quien se refieren los datos personales que sean objeto de tratamiento.

II.17 Transmisión de datos personales. La entrega total o parcial de sistemas de datos personales a cualquier persona distinta del titular de los datos, mediante el uso de medios físicos o electrónicos tales como la interconexión de computadoras o bases de datos, acceso a redes de telecomunicación, así como a través de la utilización de cualquier otra tecnología que lo permita.

III. OBJETIVO

Describir el proceso de la administración de seguridad física y las normas comprendidas en la materia, a cargo del Sistema de Agua Potable, Alcantarillado y Saneamiento del municipio de San Julián (SAPAJ), con referencia a la guía para la elaboración de un documento se seguridad del ITEI y la elaboración de especificaciones, guías, procedimientos generales, instrucciones de trabajo y registros de control.

IV.DATOS PERSONALES QUE SE RECABAN.

Los datos personales que serán sometidos a tratamiento son: nombre completo, edad, fecha de nacimiento, lugar de nacimiento, nacionalidad, estado civil, Clave Única de Registro de Población, Registro Federal de Contribuyentes. Los datos para el cumplimiento de disposiciones legales en caso de accidente o muerte: nombre de los beneficiarios, números telefónicos y referencias en caso de accidente.

V. IDENTIFICACIÓN DE LAS MEDIDAS DE SEGURIDAD

	Control	Parámetros
Medidas de seguridad Administrativas	Documentación de la política de seguridad de la información: La política de seguridad de la información debe ser aprobada por la alta gerencia, publicada y comunicada a todos los empleados y terceras partes relevantes.	En cuanto el presente documento de seguridad sea terminado, será expuesto para su aprobación y comunicada a las personas interesadas.
	Revisión de la Política de seguridad de la Información: La política de seguridad de la información debe ser revisada en intervalos planeados o si ocurren cambios significativos, para asegurar su continua aplicabilidad, adecuación y efectividad.	Cada semestre el documento de seguridad será evaluado y actualizado en caso de existir cambios significativos.
	Avisos de privacidad: Los requisitos para los avisos de privacidad o de no revelación deben reflejar las necesidades de protección de	Los avisos de privacidad serán publicados y actualizados semestralmente en caso de ser necesario a

	información de la organización y deben ser revisados periódicamente.	la par del documento de seguridad.
	Atender las necesidades de seguridad cuando se trata con ciudadanos: Todos los requisitos identificados de seguridad deben atenderse antes de dar acceso a los ciudadanos, a los activos o información de la organización.	Se realizarán la versión pública de los documentos para poder dar cumplir con los requerimientos de Trasparencia de los ciudadanos.
	Abordar la seguridad en los acuerdos de terceros: Los Acuerdos con terceros deben cubrir todos los requisitos de seguridad pertinentes, cuando estén relacionados con el acceso, tratamiento, comunicación o gestión de la información de la organización, o la adición de productos o servicios a las instalaciones de procesamiento de la información.	A los involucrados que necesiten conocer los procesos de seguridad se le dará a conocer antes del inicio de sus funciones.
	Inventarios de Activos:	Se realizará un

	Todos los activos deben ser claramente identificados y se debe elaborar y mantener un inventario de los activos más importantes.	inventario de activos y se actualizará anualmente.
	Roles y Responsabilidades: Los roles y responsabilidades de seguridad de los empleados, contratistas y usuarios de terceras partes, deben estar definidos y documentados en concordancia con la política de seguridad de la información de la organización.	En la primera capacitación se dará a conocer a los involucrados sus roles y responsabilidades sobre la seguridad de datos personales.
	Términos y Condiciones del Empleo: Como parte de su obligación contractual, los empleados, contratistas y usuarios de terceras partes, deben acordar y firmar los términos y condiciones de su contrato de empleo, el cual debe indicar su responsabilidad respecto a seguridad de la información.	Cada vez que sea contratado algún empleado nuevo, contratista o usuario de tercero se anexara a su contrato sus responsabilidades sobre los términos y condiciones respecto a la seguridad de información.
	Concienciación, Educación y Entrenamiento de Seguridad de la Información: Todos los empleados de la	En las capacitaciones que se llevaran se trataran temas sobre la Concienciación, educación sobre la Seguridad de la

	organización y, cuando sea relevante, contratistas y usuarios de terceras partes deben recibir concienciación. Asimismo, deben darse entrenamiento de forma periódica en las políticas y procedimientos organizacionales, conforme a la importancia de su función en el trabajo.	información, además de Entrenamiento sobre las medidas de seguridad, los nuevos procedimientos de respaldo y recuperación además de dar a conocer el plan de contingencia.
	Administración de Medios Removibles: Deberán documentarse e implementarse procedimientos para la gestión de medios removibles.	Cuando se implementen los Medios Removibles, se hará un manual sobre el uso de los mismos.
	Acuerdos de intercambio de información: Deberán establecerse acuerdos para el intercambio de información y aplicaciones entre la organización y entidades externas.	Se implementará la bitácora de Intercambio de Información además de las medidas de seguridad ya citadas en este documento.
	Uso Sistema de Monitoreo: Se deben establecer procedimientos para monitorear el uso de la información y los sistemas. Los resultados de las actividades de monitoreo deben ser revisados con	Las bitácoras de cada área serán implementadas para un generar un control en el uso de la información y los sistemas.

	regularidad.	
	Registro de Usuarios: Deberá existir un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas y servicio de información.	Las Bitácoras de cada área ayudara con la administración de usuarios externos al área misma, además el encargado de cada área será el responsable de la administración de acceso a los sistemas de información, así sea físicos o digitales (contraseñas, usuarios, llaves de los archiveros).
	Procedimiento de Control de Cambios: La implementación de los cambios debe ser controlada mediante el uso de procedimientos formales de control de cambios.	En caso del cambio de algún administrador de área, el nuevo encargado de la misma deberá de asegurarse de que su antecesor le entregué todas las etapas de seguridad como usuarios, contraseñas y llaves de archiveros, además de informar al encargado de la Unidad de Trasparencia con un Oficio el cumplimiento de lo anterior.
	Procedimientos y Responsabilidades de Respuesta a Incidentes de Seguridad de la Información: Se deben establecer procedimientos y responsabilidades de la administración para	En este documento de seguridad se explican los procedimientos en caso de algún incidente de Seguridad de Información, que serán explicados a los encargados de cada área, además serán

	asegurar una adecuada, ordenada y oportuna respuesta a los incidentes de seguridad.	capacitados para aplicar correctamente los procedimientos y dar a conocer cada uno sus responsabilidades sobre seguridad.
	Verificación del Cumplimiento técnico: Se deben verificar constantemente los sistemas de información para el cumplimiento de los estándares de seguridad.	En cada inventario se revisará el estado de los equipos y se actualizarán o instalarán los protocolos de seguridad adecuados.
	Distribución de las Responsabilidades de Seguridad de la Información: Todas las responsabilidades de seguridad deben estar claramente definidas.	En las capacitaciones se tratará la distribución de responsabilidades de tal manera que entren claramente definidas.
	Retorno de Activos: Todos los empleados, contratistas y usuarios de terceras partes, deben regresar a la organización todos los activos que tengan en posesión una vez termine el trabajo, contrato o acuerdo.	Todos los activos serán retornados y se llevarán a cabo las medidas de eliminación y formateo necesarios para su reutilización.
	Eliminación o Reutilización segura del equipo: Todos los artículos de equipo que contengan medios de almacenamiento deberán revisarse para asegurar la remoción o formateo apropiado de	Antes de cualquier procedimiento de Eliminación o Reutilización se llevará a cabo un formateo apropiado del equipo.

	cualquier información sensible y "software" de autor antes de su eliminación.	
Medidas de Seguridad Avanzadas para Accesos desde Red Interna RI-3 conforme a la metodología BAA del INAI.	Controles contra código malicioso: Se deberán implementar controles para la detección, prevención y recuperación de la infraestructura en contra de códigos maliciosos. Se deberán implementar procedimientos de concienciación adecuados.	Se cotizarán y se asignara un presupuesto para la instalación de un antivirus para evitar problemas con los equipos informáticos.
	Controles de Red: Las redes deben ser gestionadas y controladas con el fin de ser protegidas de las amenazas, y para mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluyendo la información en tránsito.	Actualmente no se tiene una red interna, pero se está pensando en generar una, cuando se tenga se tomarán las medidas de seguridad necesarias.
	Registro de Auditoria: Se deberán producir y almacenar registros de auditoria relacionados a las actividades de los usuarios, las excepciones, y eventos de seguridad. Estos registros deberán ser utilizados en futuras investigaciones y monitoreo de control de accesos.	Se realizarán auditorias aleatorias entre áreas para mejorar las medidas de seguridad y monitorear los controles de acceso.

	Administración de Privilegios: Deberá restringirse y controlarse la asignación y uso de privilegios.	Solamente el encargado de la unidad de transparencia tendrá la capacidad de asignar privilegios.
	Uso de Contraseñas: Se deberá exigir a los usuarios que sigan buenas prácticas de seguridad en la selección y uso de las contraseñas.	Cada equipo tendrá una contraseña segura que únicamente será conocida por el usuario de ese equipo, se seguirán las recomendaciones de contraseñas que se explican en este documento.
	Equipos Desatendidos: Los usuarios deberán asegurar que los equipos atendidos cuenten con protección adecuada.	De momento no se cuenta con equipos desatendidos, pero después de un determinado tiempo se formateará su información para que pueda ser reutilizada por otro usuario.
	Identificación y autenticación de usuarios: Todos los usuarios deben tener un identificador único para su uso personal, y una técnica de autenticación adecuada debe ser elegido para fundamentar la identidad declarada de un usuario.	De momento se utiliza cualquier documento oficial que pueda autentificar su identidad (INE, IFE, Credencial de alguna institución pública, etc.)
	Control de Vulnerabilidades Técnicas: Se debe obtener oportunamente	La bitácora de vulnerabilidades que se llevara a cabo y cuyos formatos están

	información acerca de las vulnerabilidades técnicas de los sistemas de información que se utilizan. Se debe evaluar la exposición de la organización a las mismas y se deben tomar las medidas apropiadas para enfrentar los riesgos asociados.	incluidos en este documento servirá para obtener oportunamente las vulnerabilidades técnicas y poder generar acciones para corregirlas.
Medidas de Seguridad Físicas.	Política sobre el uso de Controles Criptográficos: Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada.	En la primera capacitación se hablará sobre como encriptar documentos de Word y Excel, además se anexa un manual de cómo hacerlo en este documento.
	Respaldos de Información: Deberán realizarse copias de respaldo de la información y aplicaciones. Se deberán probar los respaldos de acuerdos a una política establecida.	Esta planeado comprarse un método de respaldo, así sea una USB, un Disco Duro y la Implementación de la nube y se realizaran respaldos periódicos para evitar la pérdida de información.
	Eliminación de los Derechos de Acceso: Los derechos de acceso de todos los empleados, contratistas y usuarios de terceras partes, a información e instalaciones de procesamiento de información deben ser	Actualmente solo los responsables de cada área tienen derecho de acceso a la información de la misma, y en caso de la contratación de nuevo personal tendrán definidos sus derechos de acceso.

	removidos en cuanto se termine el trabajo, contrato, acuerdo o cuando se requiera hacer un ajuste.	
	Perímetro de Seguridad Física: Los perímetros de seguridad (barreras, tales como paredes, tarjetas que controlan entradas o recepciones) deben ser implementados para proteger áreas que contienen información y sistemas de información.	Se está trabajando en la construcción de una pared divisoria para mejorar la protección de la oficina más vulnerable, además todos los archivos están resguardados dentro de cada área.
	Eliminación y Entrega de los Medios de Almacenamiento: Los medios deberán eliminarse de modo seguro cuando no se les necesite más, usando procedimientos formales.	Cuando se desocupen los medios de almacenamiento se utilizarán los protocolos de formateo necesarios para que puedan ser reutilizados y de destrucción apropiados antes de su eliminación.
	Medios Físicos de Almacenamiento en Transito: Cualquier medio que contenga información deberá ser protegido contra acceso no autorizado, mal uso o corrupción durante su transporte más allá de los límites de la organización.	Cuando se tenga el medio físico de almacenamiento en cada área, será resguardado bajo llave que solo posea el encargado de la misma.
Medidas Reforzadas de Seguridad para Accesos desde Entornos de Alta Anonimidad.	Controles de Red: Las redes deben ser gestionadas y	Actualmente no se tiene una red interna, pero se está pensando

	controladas con el fin de ser protegidas de las amenazas, y para mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluyendo la información en tránsito.	en generar una, cuando se tenga se tomarán las medidas de seguridad necesarias.
	Políticas y Procedimientos de Intercambio de Información: Se deberán implementar políticas, procedimientos y controles formales de intercambio para proteger la información que transite a través de cualquier tipo de instalaciones de comunicaciones.	Se implementara la bitácora de transferencia de tal manera que el intercambio de información estará controlado, además de utilizar protocolos adecuados para el intercambio de información.
	Registro de Auditoria: Se deberán producir y almacenar registros de auditoria relacionados a las actividades de los usuarios, las excepciones, y eventos de seguridad. Estos registros deberán ser utilizados en futuras investigaciones y monitoreo de control de accesos.	Se realizarán auditorias aleatorias entre áreas para mejorar las medidas de seguridad y monitorear los controles de acceso.
	Uso Sistema de Monitoreo: Se deben establecer procedimientos para monitorear el uso de la información y los	Las bitácoras de cada área serán implementadas para un generar un control en el uso de la información y los sistemas.

	sistemas. Los resultados de las actividades de monitoreo deben ser revisados con regularidad.	
	Administración de Privilegios: Deberá restringirse y controlarse la asignación y uso de privilegios.	Solamente el encargado de la unidad de transparencia tendrá la capacidad de asignar privilegios.
	Política de Uso de los Servicios de Red: Los usuarios solo deben contar con acceso a los servicios para los que han sido autorizados.	Para llevar esto acabo se utilizarán las contraseñas en los equipos de cada área de tal manera que solo el encargado de esa área pueda acceder a ellos.
	Control de Conexión de Red: Los controles de enrutamiento deben aplicarse a las redes para garantizar que las conexiones informáticas y los flujos de información no violan la política de control de acceso de las aplicaciones de negocio.	De momento no se cuenta con una red adecuada, en cuanto se implemente una se trabajará en el manual de buenas costumbres de la conexión de Red.
	Fuga de Información: Se deben prevenir las oportunidades de fuga de información.	Para evitar la fuga de documentos con datos personales, se trabajará en la capacitación para encriptar documentos de tipo Word y Excel.
	Control de Vulnerabilidades Técnicas: Se debe obtener oportunamente información acerca de las	La bitácora de vulnerabilidades que se llevara a cabo y cuyos formatos están incluidos en este

	vulnerabilidades técnicas de los sistemas de información que se utilizan. Se debe evaluar la exposición de la organización a las mismas y se deben tomar las medidas apropiadas para enfrentar los riesgos asociados.	documento servirá para obtener oportunamente las vulnerabilidades técnicas y poder generar acciones para corregirlas.
	Disociación de información cuando los datos pasen de un ambiente de riesgo menor a un ambiente de riesgo mayor.	Los respaldos se mantendrán de manera segura, para poder restaurar todos los documentos perdidos en caso de una contingencia.
	Política sobre el uso de Controles Criptográficos: Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada.	En la primera capacitación se hablará sobre como encriptar documentos de Word y Excel, además se anexa un manual de cómo hacerlo en este documento.
	Definir e implementar listas de control de acceso (ACL)	Actualmente no se tiene una red interna, pero se está pensando en generar una, cuando se tenga se tomarán las medidas de seguridad necesarias.
	Controles de DNS	Actualmente no se tiene una red interna, pero se está pensando en generar una, cuando se tenga se tomarán las medidas de seguridad

		necesarias.
	Únicamente permitir servicios públicos dentro de la DMZ.	Actualmente no se tiene una red interna, pero se está pensando en generar una, cuando se tenga se tomarán las medidas de seguridad necesarias.
	Mejores prácticas de configuración del FW.	Actualmente no se tiene una red interna, pero se está pensando en generar una, cuando se tenga se tomarán las medidas de seguridad necesarias.
	Red inalámbrica conectada a la zona desmilitarizada (DMZ) externa.	Actualmente no se tiene una red interna, pero se está pensando en generar una, cuando se tenga se tomarán las medidas de seguridad necesarias.
	Red de terceros conectada a la zona desmilitarizada (DMZ) externa.	Actualmente no se tiene una red interna, pero se está pensando en generar una, cuando se tenga se tomarán las medidas de seguridad necesarias.
	Controles de tráfico entrante y saliente	Actualmente no se tiene una red interna, pero se está pensando en generar una, cuando se tenga se tomarán las medidas de seguridad necesarias.

	Implementar y monitorear sistemas de prevención de Intrusos (IPS)	Actualmente no se tiene una red interna, pero se está pensando en generar una, cuando se tenga se tomarán las medidas de seguridad necesarias.

VI. NIVELES DE PROTECCIÓN DE LOS DATOS PERSONALES

Las medidas de seguridad que son aplicables a cada uno de los sistemas a cargo del Sistema de Agua Potable, Alcantarillado y Saneamiento del Municipio de San Julián (SAPAJ), deberán considerar el tipo de datos personales que contiene, lo cual determina el nivel de protección requerido, siendo básico, medio o alto, como a continuación se establece:

1. Nivel de protección básico:

a) **Datos de identificación**: Nombre, domicilio, estado civil, firma, RFC, CURP, lugar de nacimiento, fecha de nacimiento.

b) **Datos laborales:** Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros.

2. Nivel de protección medio:

a) **Datos patrimoniales**: Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros.

b) **Datos académicos**: Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, el Sistema de Agua Potable, Alcantarillado y Saneamiento del Municipio de San Julián (SAPAJ), debe asegurar de acuerdo con la naturaleza de los datos contenidos en los sistemas de datos personales que custodia, los niveles de protección conforme a su **grado de confidencialidad, disponibilidad e integridad**.

VII. TIPO DE TRANSMISIONES DE DATOS PERSONALES Y MODALIDADES PARA LA TRANSMISIÓN

Se deberán considerar tres **tipos de transmisiones** que se pueden llevar a cabo dependiendo de quién sea el destinatario:
a) **Interinstitucionales:** Transmisiones de datos a dependencias y entidades de la Administración Pública Federal, de los órganos Poder Judicial de la Federación, de los poderes Legislativo, Ejecutivo y Judicial locales de las entidades federativas, en el ejercicio de sus facultades.

b) **Internacionales:** Transmisiones a gobiernos de otro Estado reconocido por la comunidad Internacional y/u órganos internacionales y sus organismos, cuya competencia que motive el requerimiento haya sido reconocida por el Estado Mexicano.

c) **Con entes privados u organizaciones civiles**.

Para implementar las medidas de seguridad aplicables a las transmisiones citadas, la Unidad Administrativa responsable, debe considerar la **modalidad por la cual se envían los datos personales a los destinatarios**, pudiendo hacerse mediante el traslado de soportes físicos, mediante el traslado físico de soportes electrónicos o el traslado sobre redes electrónicas. Cada una de estas modalidades se deberá ceñir a lo siguiente:

a) **Traslado de soportes físicos**: En esta modalidad los datos personales se trasladan en medios de almacenamiento inteligibles a simple vista que no requieren de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos. Ejemplo del traslado de soportes físicos es cuando una dependencia envía por correspondencia oficios o formularios impresos.

b) **Traslado físico de soportes electrónicos:** En esta modalidad se trasladan físicamente para entregar al destinatario los datos personales en archivos electrónicos contenidos en medios de almacenamiento inteligibles sólo mediante el uso de algún aparato con circuitos electrónicos que procese su contenido para examinar, modificar o almacenar los datos. Ejemplo de ello es cuando una dependencia entrega a otra por mensajería oficial un archivo electrónico con datos

personales contenidos en discos flexibles, discos compactos o dispositivos de memoria USB, entre otros.

c) **Traslado sobre redes electrónicas**: En esta modalidad se transmiten los datos personales en archivos electrónicos mediante una red electrónica. Por ejemplo, cuando un archivo electrónico con un listado de beneficiarios se envía de una dependencia a otra por Internet.

VIII. CATÁLOGO DE SISTEMAS DE DATOS PERSONALES

Unidad Administrativa: Sistema de Agua Potable, Alcantarillado y Saneamiento del municipio de San Julián (SAPAJ).

NOMBRE	CARGO O NOMBRAMIENTO ASIGNADO	FUNCIONES
JUAN MANUEL MORALES HERNÁNDEZ	DIRECTOR DE SAPAJ	Dirección, administración y gestión del organismo SAPAJ.
KEVIN JESÚS RAMÍREZ GUTÍERREZ	SUBDIRECTOR DE SAPAJ	Asistir y suplir al director del organismo SAPAJ.
ALEJANDRA MÉNDEZ MARTÍNEZ	ENCARGADA DE FINANZAS	Encargada de llevar la cuenta pública del organismo SAPAJ
JUAN MANUEL VALLECILLO LOZANO	PADRÓN DE USUARIOS	Detección de tomas clandestinas y actualización del padrón de usuarios.

MARÍA LORENA RODRÍGUEZ ESCOBEDO	CAJA 1	Atención al usuario y cobranza.
JUAN CARPIO MUÑOZ	MAYORDOMO	Encargado del mantenimiento y operación de agua potable.
J. GUADALUPE MORENO ENRÍQUEZ	INSTALADOR DE MEDIDORES	Instalación de medidores y mantenimiento.

VIII. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE DATOS PERSONALES

Unidad Administrativa: Sistema de Agua Potable, Alcantarillado y Saneamiento del Municipio de San Julián (SAPAJ).
Nombre del sistema: Catálogo de Proveedores, Prestadores de Servicios y Usuarios.
Tipo de Soporte Tipo de soporte: Soporte Físico. Descripción Expedientes.

Características del lugar donde se resguardan los soportes: Oficina con ventilación natural, luz natural y artificial, puerta de acceso de madera y chapa, aislada de humedad, con archiveros y libreros que permiten la conservación adecuada de los documentos.
El mobiliario que contiene los expedientes se encuentra en el área física de la dirección general del Sistema de Agua Potable, Alcantarillado y Saneamiento del Municipio de San Julián (SAPAJ). Los expedientes se encuentran alojados en los archiveros los cuales están localizados junto a la PUERTA que da al exterior, la cual cuenta con protecciones metálicas, en esta área no existe consumo de alimentos, con prevención de plagas para lo cual se coloca veneno y con una temperatura ambiental media. Las oficinas mencionadas permanecen cerradas en días y horas no hábiles.

Plan de trabajo

Duración Administración 2021- 2024
Para efecto de subsanar las medidas de seguridad administrativas, técnicas y físicas, en el Sistema de Agua Potable, Alcantarillado y Saneamiento del Municipio de San Julián (SAPAJ), se

establece el siguiente Plan de Trabajo, en el cual se plantea implementar la totalidad de las medidas de seguridad faltantes en lo restante de la administración actual a partir de la aprobación del presente documento de seguridad.
En este sentido, las medidas de seguridad físicas y técnicas que requieran la erogación de recursos como la compra de muebles incombustibles, y cestos metálicos para papeles y sustitución de los materiales plásticos e inflamables, se realizarán conforme a los tiempos administrativos del Instituto y el presupuesto lo permita.

Mes 1-12

Control	Parámetro
Fuga de información: Se deben prevenir las oportunidades de fuga de información.	Determinar de manera estricta las facultades de acceso a la información de los servidores capacitados para ello.
Disociación de información cuando los datos pasen de un ambiente de riesgo menor a un ambiente de riesgo mayor.	Ninguno
Política sobre el uso de controles criptográficos: Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada.	Bloquear o dar de baja puertos y servicios innecesarios en equipos de cómputo.

Mes 12 – 24

Actividad	Áreas Involucradas
Términos y condiciones de empleo: Como parte de su obligación contractual, los empleados, contratistas y usuarios de terceras partes, deben acordar y firmar los términos y condiciones de su contrato de empleo, el cual debe indicar su responsabilidad respecto a seguridad de la información.	
Administración de medios removibles: Deberán documentarse e implementarse procedimientos para la gestión de medios removibles.	
Acuerdos de intercambio de información:	
Deberán establecerse acuerdos para el	

intercambio de información y aplicaciones entre la organización y entidades externas.	
Uso Sistema de monitoreo: Se deben establecer procedimientos para monitorear el uso de la información y los sistemas. Los resultados de las actividades de monitoreo deben ser revisados con regularidad.	
Verificación del cumplimiento técnico: Se deben verificar constantemente los sistemas de información para el cumplimiento de los estándares de seguridad.	
Distribución de las responsabilidades de seguridad de la información: Todas las responsabilidades de seguridad deben estar claramente definidas.	

Mes 24 al Termino de la Administración 2021- 2024

Control	Parámetro
Eliminación de los derechos de acceso: Los derechos de acceso de todos los empleados, contratistas y usuarios de terceras partes, a información e instalaciones de procesamiento de información deben ser removidos en cuanto se termine el trabajo, contrato, acuerdo o cuando se requiera hacer un ajuste.	Dirección de Protección de Datos Personales, Coordinación de Planeación y Dirección de Administración.
Eliminación y entrega de los medios de almacenamiento: Los medios deberán eliminarse de modo seguro cuando no se les necesite más, usando procedimientos formales.	Dirección de Protección de Datos Personales, Coordinación de Planeación y Dirección de Administración.
Elaboración del Plan de Contingencia.	Todas las Áreas.