

**DOCUMENTO DE SEGURIDAD DEL SISTEMA DE LOS SERVICIOS DE AGUA  
POTABLE, DRENAJE Y ALCANTARILLADO DE PUERTO VALLARTA.  
(19-MARZO-2019)**

El presente documento contiene las disposiciones en materia de Protección de Datos Personales en las diversas áreas de este Sistema de los Servicios de Agua Potable, Drenaje y Alcantarillado de Puerto Vallarta en las que se genera, posee o administra información.

**CONTENIDO:**

I.- DEFINICIONES.

II.-SISTEMAS DE DATOS

III.-NIVELES DE PROTECCIÓN DE LOS DATOS PERSONALES

IV.-DATOS PERSONALES CONTENIDOS EN LOS SISTEMAS

V.-FUNCIONES Y OBLIGACIONES DE LOS SERVIDORES PÚBLICOS AUTORIZADOS PARA ACCEDER, MANEJAR Y CUSTODIAR LOS DATOS PERSONALES (ENCARGADOS).

VI.-TIPOS DE MEDIDAS DE SEGURIDAD

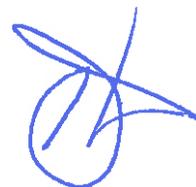
VII.-PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS.

VIII.-TRANSFERENCIA DE DATOS PERSONALES

IX.- BITÁCORAS DE ACCESO, OPERACIÓN COTIDIANA Y VULNERACIONES A LA SEGURIDAD DE DATOS PERSONALES.

X.- TÉCNICAS DE SUPRESIÓN Y BORRADO SEGURO DE DATOS PERSONALES.

XI.- PLAN DE TRABAJO



## PRESENTACIÓN:

En su artículo 30 la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados en el Estado de Jalisco establece que: 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; sin perjuicio de lo establecido por las disposiciones vigentes en materia de seguridad emitidas por las autoridades competentes al sector que corresponda; asimismo, la misma Ley en su artículo 34 señala lo siguiente: Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión

Por lo anterior, para el Sistema de los Servicios de Agua Potable, Drenaje y Alcantarillado de Puerto Vallarta, la información Personal es un activo que debe protegerse mediante un conjunto de procesos y sistemas diseñados, administrados y mantenidos por el personal que los resguarda; 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 el Organismo afronta según lo establecido por la Ley de la materia.

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

Este Documento tiene como fin la homogeneidad en la organización, procesos y sistemas, en el que el Comité de Transparencia, conjuntamente con el área de Informática y los responsables de los datos personales, definen las medidas de seguridad administrativa y física implementadas para la protección de los sistemas de datos personales custodiados.

El presente Documento de Seguridad es aplicable y de observancia obligatoria para todas las Unidades Administrativas del Sistema de los Servicios de Agua Potable, Drenaje y Alcantarillado de Puerto Vallarta, en cumplimiento a las funciones que le son inherentes, así como por todos los individuos que pertenezcan a esta dependencia sea cual fuere su nivel jerárquico y su situación en la misma; así como para las personas externas que debido a la presentación de un servicio, tengan acceso a tales sistemas o al sitio donde se ubican los mismos.

## I- DEFINICIONES.

**Áreas:** Instancias internas del Sistema de los Servicios de Agua Potable, Drenaje y Alcantarillado de Puerto Vallarta, que cuentan o puedan contar, dar tratamiento, y ser responsables o encargadas de los datos personales;

**Aviso de privacidad:** Documento físico y electrónico que es puesto a disposición del titular con el objeto de informarle los propósitos principales del tratamiento al que serán sometidos sus datos personales por parte de esta dependencia.

**Bases de Datos:** Conjunto ordenado de los datos personales referentes a una persona física identificada o identificable, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

**Bloqueo:** La identificación y conservación de los 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 correspondiente.

**Comité de Transparencia:** El Comité de Transparencia del Sistema de los Servicios de Agua Potable, Drenaje y Alcantarillado de Puerto Vallarta, conformado según lo establecido por la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.

**Datos personales:** Cualquier información concerniente a una persona física 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:** Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud, información genética, datos biométricos, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

**Encargado:** Persona física o jurídica, que sola o conjuntamente con otras, trata datos personales a nombre y por cuenta del responsable;

**Incidente:** Es el robo o extravío de los datos personales en posesión de una unidad administrativa o una incursión de una persona no autorizada al sistema de datos personales.

**Remisión:** toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado.



**Responsable:** El servidor Público Titular de la Unidad Administrativa que decide sobre el tratamiento físico o automatizado de datos personales, así como el contenido y finalidad de los sistemas de datos personales.

**Sistema de datos personales (SDP):** Es el conjunto ordenado de datos personales que están en posesión de la dependencia, con independencia de su forma de acceso, creación, almacenamiento u organización.

Los sistemas de datos personales son:

- a) **Físicos:** Conjunto de datos que para su tratamiento están ordenados en registros manuales, impresos, sonoros, magnéticos o visuales.
- b) **Automatizados:** Conjunto ordenado de datos que para su tratamiento has sido o están sujetos a un tratamiento informático, y que requieren de una herramienta tecnológica específica para su acceso, recuperación o tratamiento.

**Supresión:** La baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable.

**Titular:** Persona física a quien pertenecen los datos personales;

**Transferencia:** Toda entrega total o parcial del sistema de datos personales realizada por la institución a cualquier persona distinta al Titular de los datos, mediante el uso de medios físicos o electrónicos.

**Tratamiento:** Operaciones y procedimientos físicos o automatizados que permitan recabar, registrar, reproducir, conservar, organizar, modificar transmitir y cancelar datos personales.

**Unidad de Transparencia:** instancia que funge como vínculo entre el responsable y el titular.

**Usuario:** Servidor Público facultado por un Instrumento Jurídico o expresamente autorizado por el Responsable que utiliza de manera cotidiana datos personal para el ejercicio de sus atribuciones, por lo que accede a los sistemas de datos personales, sin posibilidad de agregar o modificar su contenido.

## II.-SISTEMAS DE DATOS

<b>Unidad Administrativa: Oficialía de Partes</b>	
<b>Nombre del sistema:</b>	Sistema de los Servicios de Agua Potable, Drenaje y Alcantarillado de Puerto Vallarta.
<b>Responsable:</b>	
<b>Nombre:</b>	Ing. Francisco Javier Rojas Gómez
<b>Cargo:</b>	Director General
<b>Funciones:</b>	Dirigir el funcionamiento y cumplimiento de las actividades del Organismo, asegurándose de que sean las adecuadas para lograr la finalidad de restar, administrar, conservar y mejorar los servicios de agua potable, drenaje y alcantarillado de Puerto Vallarta, de acuerdo a los planes establecidos por el Gobierno Federal, Estatal y Municipal en beneficio de la comunidad de Puerto Vallarta.
<b>Obligaciones:</b>	Vigilar que se lleve a cabo el resguardo de datos personales conforme a lo establecido en las Leyes de la materia
<b>Encargados:</b>	
<b>Nombre(l):</b>	María Guadalupe Quirarte Palomera
<b>Cargo:</b>	Coordinadora de la Oficialía de Partes.
<b>Funciones:</b>	<ul style="list-style-type: none"> <li>• Atención de llamadas telefónicas para el Director</li> <li>• Mantener la agenda de citas del Director, así como llevar un control interno de las personas que atiende</li> <li>• Dar seguimiento a diferentes asuntos del Organismo</li> <li>• Revisar documentación ingresada</li> <li>• Seguimiento de asuntos de usuarios</li> </ul>
<b>Obligaciones:</b>	Supervisar el correcto resguardo de datos personales conforme a lo establecido en las Leyes de la materia.

<b>Unidad Administrativa: Atención a usuarios</b>	
<b>Nombre del sistema:</b>	Sistema de los Servicios de Agua Potable, Drenaje y Alcantarillado de Puerto Vallarta.
<b>Responsable:</b>	
<b>Nombre:</b>	Lic. Brenda María Peña Cárdenas
<b>Cargo:</b>	Jefa del Departamento de Atención a Usuarios
<b>Funciones:</b>	<ul style="list-style-type: none"> <li>• Representar Sistema de los Servicios de Agua Potable, Drenaje y Alcantarillado de Puerto Vallarta ante los usuarios, así como resolver cuestiones derivadas del propio Organismo.</li> <li>• Supervisar la efectividad del servicio en Conmutador atendiendo con oportunidad las solicitudes y quejas recibidas</li> </ul>

Obligaciones:	Vigilar que se lleve a cabo el resguardo de datos personales conforme a lo establecido en las Leyes de la materia
<b>Encargados:</b>	
Nombre(1):	María Guadalupe Nava Becerra
Cargo:	Jefe de Sección
Funciones:	<ul style="list-style-type: none"> <li>• Analizar, investigar y verificar estudios socioeconómicos de los usuarios de escasos recursos.</li> <li>• Atención al público en general y satisfacer sus necesidades.</li> </ul>
Obligaciones:	Supervisar el correcto resguardo de datos personales conforme a lo establecido en las Leyes de la materia.

Nombre(2):	Lic. Salma Yamile Tarabay Orozco
Cargo:	Encargada de oficina Unirse
Funciones:	<ul style="list-style-type: none"> <li>• Representar Sistema de los Servicios de Agua Potable, Drenaje y Alcantarillado de Puerto Vallarta ante los usuarios, así como resolver cuestiones derivadas del propio Organismo.</li> <li>• Supervisar la efectividad del servicio en Conmutador atendiendo con oportunidad las solicitudes y quejas recibidas</li> </ul>
Obligaciones:	Supervisar el correcto resguardo de datos personales conforme a lo establecido en las Leyes de la materia.

Nombre(3):	Lic. Susana Roció Ortega Arias
Cargo:	Encargada de oficina Ixtapa
Funciones:	<ul style="list-style-type: none"> <li>• Representar Sistema de los Servicios de Agua Potable, Drenaje y Alcantarillado de Puerto Vallarta ante los usuarios, así como resolver cuestiones derivadas del propio Organismo.</li> <li>• Supervisar la efectividad del servicio en Conmutador atendiendo con oportunidad las solicitudes y quejas recibidas</li> </ul>
Obligaciones:	Supervisar el correcto resguardo de datos personales conforme a lo establecido en las Leyes de la materia.

Nombre(4):	Ángel Nicolas Urrutia González
Cargo:	Encargado de oficina Pitillal

310

4

Funciones:	<ul style="list-style-type: none"> <li>• Representar Sistema de los Servicios de Agua Potable, Drenaje y Alcantarillado de Puerto Vallarta ante los usuarios, así como resolver cuestiones derivadas del propio Organismo.</li> <li>• Supervisar la efectividad del servicio en Conmutador atendiendo con oportunidad las solicitudes y quejas recibidas</li> </ul>
Obligaciones:	Supervisar el correcto resguardo de datos personales conforme a lo establecido en las Leyes de la materia.

Nombre(5):	Irma Zavala Pedraza
Cargo:	Encargada de oficina Coapinole
Funciones:	<ul style="list-style-type: none"> <li>• Representar Sistema de los Servicios de Agua Potable, Drenaje y Alcantarillado de Puerto Vallarta ante los usuarios, así como resolver cuestiones derivadas del propio Organismo.</li> <li>• Supervisar la efectividad del servicio en Conmutador atendiendo con oportunidad las solicitudes y quejas recibidas</li> </ul>
Obligaciones:	Supervisar el correcto resguardo de datos personales conforme a lo establecido en las Leyes de la materia.

<b>Unidad Administrativa:</b> Catastro a Usuarios	
Nombre del sistema:	Sistema de los Servicios de Agua Potable, Drenaje y Alcantarillado de Puerto Vallarta.
<b>Responsable:</b>	
Nombre:	Lic. Adalberto Gregorio Velázquez Vaca
Cargo:	Jefe del Departamento de Catastro a Usuarios
Funciones:	<ul style="list-style-type: none"> <li>• Dictaminar los montos a cobrar por contratos, consumos mínimos omitidos así como</li> <li>• la tipificación de infracciones y multas en base a la ley. (R)</li> <li>• • Clasificación del tipo de contrato a aplicar en base a los datos recabados en el</li> <li>• estudio catastral, sea comercial, domestico o industrial. (R)</li> <li>• • Suscribir contratos y convenios, para establecer obligaciones y derechos entre</li> <li>• Usuarios y el Organismo. (R)</li> <li>• • Supervisión y coordinación de las actividades del personal. (R)</li> </ul>

*3/10*

*f*

	<ul style="list-style-type: none"> <li>• Aplicación y cálculo de multas a infractores. (R)</li> <li>• Atención personalizada a usuarios morosos para convenio de facturación,</li> <li>• reestructuración de adeudos. (R)</li> <li>• Gestionar soluciones a problemas que influyen en la contratación o sanción de un</li> <li>• usuario. (P)</li> </ul>
Obligaciones:	Vigilar que se lleve a cabo el resguardo de datos personales conforme a lo establecido en las Leyes de la materia

<b>Encargados:</b>	
Nombre(l):	C. Elsa Yudith Razo Zamorano
Cargo:	Auxiliar de Área
Funciones:	<ul style="list-style-type: none"> <li>• Atender a los usuarios para realizar su contrato.</li> <li>• Revisar documentación de los usuarios para elaborar contrato.</li> <li>• Revisión de nuevos contratos con documentación anexa.</li> <li>• Coordinación con el personal de catastro para elaboración de nuevos contratos, cambios de propietario, certificados de no adeudo, cambios de clasificación.</li> <li>• Elaboración de oficios e informes para cambios de clasificación, corrección de datos, etc.</li> </ul>
Obligaciones:	Supervisar el correcto resguardo de datos personales conforme a lo establecido en las Leyes de la materia.

<b>Encargados:</b>	
Nombre(l):	C. Marcela Ramos Hernández
Cargo:	Auxiliar de Área
Funciones:	<ul style="list-style-type: none"> <li>• Atender a los usuarios para realizar su contrato.</li> <li>• Revisar documentación de los usuarios para elaborar contrato.</li> <li>• Revisión de nuevos contratos con documentación anexa.</li> <li>• Coordinación con el personal de catastro para elaboración de nuevos contratos, cambios de propietario, certificados de no adeudo, cambios de clasificación.</li> <li>• Elaboración de oficios e informes para cambios de clasificación, corrección de datos, etc.</li> </ul>
Obligaciones:	Supervisar el correcto resguardo de datos personales conforme a lo establecido en las Leyes de la materia.

### III.-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 los Servicios de Agua Potable, Drenaje y Alcantarillado de Puerto Vallarta, se 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, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros.
- 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 sobre procedimientos administrativos seguidos en forma de juicio y/o procesos jurisdiccionales:** Información relativa a una persona que se encuentre sujeta como parte o tercero en torno a un procedimiento administrativo seguido en forma de juicio o proceso jurisdiccional en materia laboral, civil, familiar, penal, de justicia para adolescentes, amparo o administrativa, con independencia de su etapa de trámite
- c) **Datos académicos:** Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros.
- d) **Datos de tránsito y movimientos migratorios:** Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.

#### 3. Nivel de protección alto:

- a) **Datos ideológicos:** Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y asociaciones religiosas, entre otros.
- b) **Datos de salud:** Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas,

consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos y prótesis, entre otros.

- c) **Características personales:** Tipo de sangre, ADN, huella dactilar u otros análogos.
- d) **Características físicas:** Color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros.
- e) **Vida sexual:** Preferencia sexual, hábitos sexuales, entre otros.
- f) **Origen:** Étnico y racial.

El Sistema de los Servicios de Agua Potable, Drenaje y Alcantarillado de Puerto Vallarta, a través de las Unidades Administrativas, 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.**



#### IV.-DATOS PERSONALES QUE PUDENE O NO ESTAR CONTENIDOS EN LOS SISTEMAS O BASES.

- Nombre.
- Dirección.
- Correo electrónico.
- Número telefónico.
- Datos patrimoniales o información financiera, como cuentas bancarias, número de tarjeta de crédito, bienes inmuebles, deudas por servicios de agua, drenaje y accesorios.
- Identificación oficial.
- RFC.
- Firma autógrafa.
- De los trabajadores, datos laborales como información curricular, grado de estudios, información sobre cónyuge o hijos, CURP.

#### V.- FUNCIONES Y OBLIGACIONES DE LOS SERVIDORES PÚBLICOS AUTORIZADOS PARA ACCEDER, MANEJAR Y CUSTODIAR LOS DATOS PERSONALES (ENCARGADOS).

##### Funciones:

- Verificar que el sistema de datos personales se encuentre completo y sin alteraciones.
- Llevar un registro de los Servidores Públicos, que previa autorización acceden al sistema de datos personales.
- Actualizar trimestralmente la relación de usuarios que acceden al sistema de datos personales.
- Informar al responsable sobre transmisiones parciales o totales de datos personales y llevar el registro.
- Informar al responsable del sistema sobre los incidentes que ocurran y llevar el registro.

##### Obligaciones:

- Proponer mecanismos para asegurar que los datos personales en posesión de la Unidad Administrativa, en el ejercicio de sus facultades, no se difundan, distribuyan o se haga mal uso de ellos.
- Garantizar la seguridad de los datos personales y evitar su alteración, pérdida, transmisión y acceso no autorizado.



## VI.-TIPOS DE MEDIDAS DE SEGURIDAD

**Medidas De Seguridad Administrativas.-** Estas atañen a las políticas de seguridad, cumplimiento de la normatividad aplicable, organización de la seguridad de la información, clasificación y control de activos, seguridad relacionada con recursos humanos, administración de incidentes.

### **Medidas de seguridad administrativas implementadas:**

Se utilizan y custodian los datos personales únicamente en las áreas administrativas que corresponde.

Los datos personales que se recaban en los sistemas de Tratamiento únicamente son accesibles al personal facultado para ello, según lo establezcan las leyes de la materia, y en su caso si se desprende de las facultades para las que fueron contratados.

Los datos personales recabados, son tratados únicamente para las finalidades para las que fueron recabados.

El aviso de privacidad corto de la dependencia, se pone siempre a la vista del titular, indicándole de qué manera se puede consultar el integral, y de no haber manifestación en contrario, se entenderá que acepta los términos del mismo de manera tacita.

**Medidas de Seguridad Físicas.-**Atañen a las acciones que deben implementarse para contar con:

- **Seguridad física y ambiental.** Establecimiento de controles relacionados con los perímetros de seguridad física y el entorno ambiental de los datos, con el fin de prevenir accesos no autorizados, daños, robo, entre otras amenazas. Se enfoca en aspectos tales como los controles implementados para espacios seguros y seguridad del equipo.

### **Medidas de seguridad física implementadas:**

En primer término, los trabajadores dependientes de este Organismo, sea cual fuere su estatus, deben portar gafete de identificación que contenga nombre, cargo, vigencia, firma del titular de la institución, domicilio de la institución, teléfono de la institución, con el cual podrán comprobar que están autorizados para el manejo de los datos personales.

Toda persona ajena que tenga acceso a la dependencia debe proporcionar sus datos registrándose en la entrada, con lo cual se le otorga un gafete identificándolo como visitante del Organismo.

Cada una de las áreas cuenta con espacios restringidos al acceso de visitantes, para evitar el contacto de estos con los expedientes y/o cualquier sistema de datos personales.

Todas las computadoras precisarán de un nombre de usuario y contraseña para ingresar, mismos que son actualizados de manera periódica, para evitar vulneraciones a los sistemas.

Se vigila constantemente mediante el monitoreo de cámaras todas las aéreas del Organismo, para que en el caso de que se presente algún incidente poder determinar las acciones a tomar en el área encargada.

Queda prohibido al personal de la dependencia, así como a visitantes, el uso de cualquier artefacto que pueda provocar daño a los expedientes y equipo.

**Medidas de seguridad técnicas** Son las aplicables a sistemas de datos personales en soportes electrónicos servicios e infraestructura de telecomunicaciones y tecnologías de la información.

#### Medidas de seguridad técnicas

Se implementa antivirus en cada uno de los equipos de cómputo con los que cuenta el Organismo, para el efecto de que no sufran daño informático que pongan en riesgo los activos en materia de Datos Personales.

Los controles de acceso a equipos de cómputo son protegidos con contraseñas que son únicamente otorgadas al personal autorizado para el uso exclusivo de ese equipo, con la finalidad de que no se irrumpa por parte de terceros al sistema de datos.

Se realiza la gestión de telecomunicaciones para el efecto de Identificar, clasificar y evaluar las incidencias con la implementación de acciones de mejora para lograr el rendimiento óptimo en la operación de los servicios para las redes de comunicación interna.

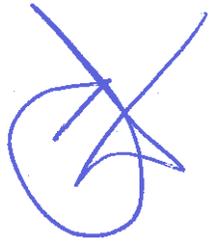
Seguridad perimetral con sistema firewall, con la finalidad de detectar y prevenir y detener amenazas de sistemas externos, que puedan causar daños y o perdida de información de los sistemas internos.



## VII.-PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS.

Se realiza mediante un servidor appliance, en el cual se respalda toda la información de los activos resguardados de manera general de la dependencia.

Se cuenta con equipos de respaldo de energía (no brake), para el caso de alguna eventualidad de falta de energía eléctrica, los equipos se mantienen encendidos, con la posibilidad de realizar el resguardo de información previo y adecuado.



## VIII.-TRANSFERENCIA DE DATOS PERSONALES

Se deberán considerar tres tipos de transferencias 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 Estatal, 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 transferencias 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 ciñe a lo siguiente:

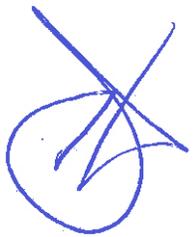
- a) **Transferencias en soportes físicos:** En esta modalidad los datos personales se trasladan en medios de almacenamiento inteligibles a simple vista que no requieren de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos. Ejemplo: por correspondencia, oficios o formularios impresos, notificaciones personales, para estos casos, el área responsable deberá siempre hacer del conocimiento del destinatario que se le transfieren datos personales, por lo que se deberán tomar las medidas necesarias conforme a la Ley de la materia, asimismo los paquetes que contengan datos personales, deberán viajar debidamente cerrados y sellados de forma tal que sea perceptible cualquier violación a los mismos; la entrega de documentos se realizará solo si el destinatario acredita su identidad para ello, el destinatario entrega una identificación oficial, y el poseedor de la información deberá recabar nombre, forma y número de referencia de la identificación, además de la fecha de entrega.

El transmisor verifica que el mensajero y/o notificador, haya entregado el paquete o documento al destinatario, si el transmisor detecta que el paquete fue entregado a otra persona, dará inicio al proceso de atención a un incidente.

- b) **Transferencias físicas de soportes electrónicos:** En esta modalidad se trasladan físicamente para entregar al destinatario previa identificación, 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 archivos electrónicos con datos personales contenidos en discos flexibles, discos compactos o dispositivos de memoria USB, entre otros; sin embargo al igual que en el caso anterior, el área responsable deberá hacer del conocimiento de destinatario que se proporcionan datos personales y las medidas necesarias para el tratamiento de los mismos.

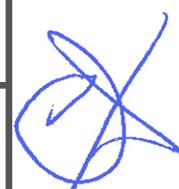
- c) **Transferencia sobre redes electrónicas:** En esta modalidad se transmiten los datos personales en archivos electrónicos mediante una red electrónica, tomándose las medidas de seguridad técnicas relacionadas a los soportes electrónicos servicios e infraestructura de telecomunicaciones y tecnologías de la información



**IX.- INCIDENCIAS Y BITÁCORAS DE ACCESO, OPERACIÓN COTIDIANA Y VULNERACIONES A LA SEGURIDAD DE DATOS PERSONALES.**

- **Bitácoras de acceso.**

<b>NOMBRE:</b>	
<b>CARGO:</b>	
<b>EXPEDIENTE O DOCUMENTO:</b>	
<b>FOJAS:</b>	
<b>PROPÓSITO DE ACCESO:</b>	
<b>FECHA DE ACCESO:</b>	
<b>HORA DE ACCESO:</b>	
<b>FECHA DE DEVOLUCIÓN:</b>	
<b>HORA DE DEVOLUCIÓN:</b>	



- Bitácoras de vulneraciones a la seguridad de los datos personales.

<b>NOMBRE DE QUIEN REPORTA:</b>	
<b>CARGO DE QUIEN REPORTA:</b>	
<b>FECHA EN LA QUE OCURRIÓ:</b>	
<b>MOTIVO DE LA VULNERACIÓN:</b>	

Una incidencia puede ser:

Cualquier incumplimiento de las normas desarrolladas en el Documento de Seguridad

Cualquier anomalía que afecte o pueda afectar a la seguridad de los datos de carácter personal en el Sistema.

Las incidencias deben ser documentadas para delimitar responsabilidades, estableciendo procedimientos que cuenten con un registro.





## X.- TÉCNICAS DE SUPRESIÓN Y BORRADO SEGURO DE DATOS PERSONALES.

Métodos Físicos 1. Trituración mediante corte cruzado o en partículas: Cortar el documento de forma vertical y horizontal generando fragmentos diminutos, denominados "partículas", lo cual hace prácticamente imposible que se puedan unir.

2. Destrucción de los medios de almacenamiento electrónicos mediante desintegración, consistente en separación completa o pérdida de la unión de los elementos que conforman algo, de modo que deje de existir. Métodos Lógicos

3. Sobre-escritura: consiste en sobrescribir todas las ubicaciones de almacenamiento utilizables en un medio de almacenamiento, es decir, se trata de escribir información nueva en la superficie de almacenamiento, en el mismo lugar que los datos existentes, utilizando herramientas de software.

4. La desmagnetización, la destrucción y la sobre escritura en la totalidad del área de almacenamiento de la información.



## XI.- PLAN DE TRABAJO.-

En este aparatado se deben incluir los elementos faltantes del Documento de Protección de Datos Personales, y el plan de trabajo para subsanar las áreas de oportunidad encontradas, así como la temporalidad en que se subsanarán los elementos faltantes:

<b>Análisis de riesgos</b>	Los Lineamientos Generales de Protección de Datos Personales, establecen los puntos a considerar para realizar el análisis de riesgo contenido en el documento de seguridad, por lo que este Organismo continua en el procedimiento de establecer dichos puntos, para así en el término no mayor a seis meses, establecer un análisis de riesgos adecuado a los sistemas de tratamiento de esta dependencia.
<b>Mecanismos de monitoreo y medidas de seguridad.</b>	Aquí se deben señalar las acciones que se deben tomar para mantener actualizadas las medidas de seguridad, describiendo la forma en que se llevarán a cabo y la temporalidad que tendrán, por lo que en el periodo de tiempo de la presente administración Institucional, se hará el informe correspondiente a dichos mecanismos.
<b>Análisis de brecha</b>	La realización de una análisis de brecha va enfocado a la seguridad de los datos personales recabados, realizando un diagnóstico de las prácticas de seguridad de la información con la que se cuenta en este momento en contraste con las que deberían tenerse en las mejores prácticas, por lo que se trabajara en el mejoramiento de la seguridad institucional, activos del responsable, seguridad e recursos humanos, seguridad física y ambiental, operación procedimientos y comunicación, cumplimiento con leyes y lineamientos, control de acceso a la información, seguridad en los sistemas

*Handwritten signatures and initials in blue ink.*

	de la información, y la prevención de los incidentes que puedan resultar en la dependencia.
--	---

**APROBACIÓN DEL DOCUMENTO DE SEGURIDAD**

---

**Responsable del desarrollo:**

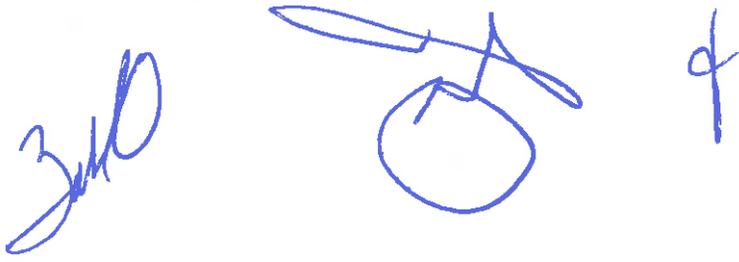
**LIC. OMAR EVERARDO LOPEZ AGUILAR, EN SU CARÁCTER DE ANALISTA DE TRANSPARENCIA, QUIEN ACTÚA COMO ENCARGADO DE LLEVAR TODO LO REFERENTE AL TEMA DE TRANSPARENCIA.**

**Revisó:**

**LIC. BIANCA ISADORA GOMEZ ONTIVEROS, EN SU CARÁCTER DE TITULAR DE LA UNIDAD DE TRANSPARENCIA DEL SISTEMA DE LOS SERVICIOS DE AGUA POTABLE DRENAJE Y ALCANTARILLADO DE PUERTO VALLARTA.**

**Autorizó:**

**COMITÉ DE TRANSPARENCIA DEL SISTEMA DE LOS SERVICIOS DE AGUA POTABLE DRENAJE Y ALCANTARILLADO DE PUERTO VALLARTA.**



Three handwritten signatures in blue ink are present below the text. The first signature on the left is a stylized 'Z' or 'M' shape. The middle signature is a large, circular loop with a horizontal line extending to the left. The third signature on the right is a simple, vertical 'd' shape.



A handwritten signature in blue ink, consisting of a large, circular loop with a horizontal line extending to the right.

