

DOCUMENTO DE SEGURIDAD

EN MATERIA DE TRATAMIENTO DE DATOS PERSONALES EN
POSESIÓN DE LA COMISION ESTATAL DE AGUA POTABLE Y
ALCANTARILLADO DE SINALOA.

Contenido

I. Introducción	4
II. Marco Normativo	6
IV. Política de Protección de Datos Personales de la Comisión Estatal de Agua Potable y Alcantarillado de Sinaloa	8
Objeto.	8
A. Responsable del Tratamiento de los Datos Personales y Fundamento para ello. 8	
B. Datos Sometidos a Tratamiento	8
C. Derechos de los Titulares de los Datos Personales	10
D. Área responsable de la implementación y observancia de esta política.	10
E. Autorización – Consentimiento	11
F. Seguridad de los Datos Personales	12
G. Tratamiento de Datos Personales	13
V. Funciones y Obligaciones del personal involucrado en el tratamiento de datos personales	14
VI. Inventarios de Datos Personales y de los Sistemas de Tratamiento	14
Dirección Administrativa.	16
Dirección Normativa	20
Dirección Técnica	24
Dirección Licitaciones y Contratos	29
VII. Medidas de Seguridad	34
VIII. Análisis de Riesgos	38
IX. Análisis de Brecha.	40
X. Plan de Trabajo.	40
XI. Metodología para la redacción y vinculación de la información	40
Dirección Administrativa.	41
1. Medidas de Seguridad actuales	41
2. Análisis de Riesgos	42
3. Análisis de Brecha	42
4.- Plan de Trabajo	43

Dirección de Normatividad	44
1. Medidas de Seguridad actuales	44
2. Análisis de Riesgos:	45
3. Análisis de Brecha:	46
4.- Plan de Trabajo	46
Dirección Técnica.....	47
1. Medidas de Seguridad actuales	47
2. Análisis de Riesgos:	48
3. Análisis de Brecha:	48
4.- Plan de Trabajo	49
Dirección de Licitaciones y Contratos.....	50
1. Medidas de Seguridad actuales	50
2. Análisis de Riesgos:	51
3. Análisis de Brecha:	52
4.- Plan de Trabajo	53
XII. Mecanismos de Monitoreo.....	54
XIII. Programa General de Capacitación	54
XIV. Actualizaciones	55
Aprobación	55

I. Introducción.

El derecho de acceso y rectificación de los datos personales en el Estado de Sinaloa encuentra su antecedente en la Ley de Acceso a la Información Pública del Estado de Sinaloa, publicada en el año 2002.

El 20 de Julio de 2007, se reforma el artículo 6 de la Constitución Política de los Estados Unidos Mexicanos, en la cual se reconoce el derecho de acceso a la información como una garantía fundamental, las fracciones II y III tienen la virtud de ser las primeras menciones constitucionales expresas que hacen un reconocimiento del derecho a la protección de datos personales y se constituyen como limitantes al ejercicio del derecho de acceso a la información.

El 2009 se distingue por, la concreción de dos relevantes acontecimientos relacionados con la consolidación del derecho a la protección de datos en México, la aprobación de las reformas a los artículos 16 y 73 de la Constitución.

El artículo 16 constitucional incorpora a la lista de garantías fundamentales consagradas en nuestra Carta Magna, el derecho a la protección de datos personales y lo dota de contenido, a saber: *“Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros”*

Por su parte, el artículo 73 constitucional dota de facultades al Congreso de la Unión para legislar en materia de protección de datos personales en posesión de particulares.

El 13 de abril de 2010, la Cámara de Diputados aprobó el proyecto de decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de

los Particulares, por su parte, la Cámara de Senadores aprobó por unanimidad dicho dictamen, el 27 de abril de 2010 y finalmente, el 5 de julio de 2010 el Poder Ejecutivo Federal publicó en el Diario Oficial de la Federación la Ley.

El 26 de Julio de 2017 se publica la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Sinaloa (LPDPPSOES), la cual entro en vigor al día siguiente de su publicación.

El 15 de Marzo de 2019, la Comisión Estatal para Acceso a la Información Pública, publicó el acuerdo mediante el cual se aprueba los Lineamientos de Protección de Datos Personales para Sujetos Obligados del Estado de Sinaloa.

A partir de la publicación de la LPDPPSOES y los Lineamientos de Protección de Datos Personales para Sujetos Obligados del Estado de Sinaloa, Comisión Estatal de Agua Potable y Alcantarillado de Sinaloa (CEAPAS) adquiere el carácter de “Responsable” y deberá tratar dichos datos conforme a los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad; adoptar medidas de seguridad para la protección de los mismos; plasmar un documento de seguridad de dichas medidas, garantizar los derechos de acceso, rectificación , cancelación y oposición.

Entre los “Deberes” previstos en la LPDPPSOES, la CEAPAS 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, para lo cual la Dirección de Políticas de Transparencia coordinó la elaboración de este documento.

II. Marco Normativo.

Para efectos de este documento, la normatividad aplicable es la siguiente:

- Artículos 6 y 16 de la Constitución Política de los Estados Unidos Mexicanos.
- Ley General de Transparencia y Acceso a la Información Pública (LGTAIP).
- Ley General de Protección de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO).
- Ley de Transparencia y Acceso a la Información Pública del Estado de Sinaloa (LTAIPES).
- Ley Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Sinaloa (LPDPPSOES).
- Reglamento Interior de la Comisión Estatal de Agua Potable y Alcantarillado de Sinaloa.
- Lineamientos de Protección de Datos Personales para Sujetos Obligados del Estado de Sinaloa.

III. Ámbito de aplicación.

En atención a los “Deberes” que refiere la LPDPSOES, el presente documento es aplicable para todas las áreas de la CEAPAS, que en el ejercicio de sus atribuciones y funciones, administren bases de datos en sistemas de tratamiento de datos personales, que tengan acceso a soportes físicos y/o electrónicos, con independencia de la forma o modalidad de su creación, procesamiento, almacenamiento y organización. Los datos personales podrán ser expresados en forma numérica, alfabética, grafica, alfanumérica, fotográfica, acústica o cualquier formato que haga identificable a una persona.

IV. Política de Protección de Datos Personales de la Comisión Estatal de Agua Potable y Alcantarillado de Sinaloa.

La CEAPAS, protegerá los datos personales proporcionados a ésta, en base a lo dispuesto en la LPDPPSOES y los Lineamientos de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Sinaloa.

Objeto.

La Política de Protección de Datos Personales explica cómo se tratan y protegen los Datos Personales que sean recolectados por esta comisión, en todas sus bases de datos y/o archivos que contengan Datos Personales.

A. Responsable del Tratamiento de los Datos Personales y Fundamento para ello.

Conforme lo dispuesto en la LTAIPES y en la LPDPPSOES, la CEAPAS es la responsable del tratamiento de los datos personales que le proporcionen, y el fundamento para tratar sus datos personales, se encuentra en los artículos 21, 94, 165 y el segundo párrafo del artículo 166 de la LTAIPES y en los artículos 1, 2, 3, 4 fracción II, 14, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 196 fracción VIII de la LPDPPSOES y el artículo 26 fracción I, XXII, XL del Reglamento Interior de la Comisión Estatal de Agua Potable y Alcantarillado de Sinaloa.

B. Datos Sometidos a Tratamiento.

Los datos personales serán utilizados con la finalidad de:

- a) Expediente único de personal, a fin de realizar los trámites administrativos y fiscales.
- b) Identificar a la persona que comparece a la celebración de la audiencia de ley en el procedimiento administrativo disciplinario, así como a las personas y testigos que intervienen en la entrega y recepción de las oficinas públicas del poder Ejecutivo del Estado y expedir la constancia de no inhabilitación en materia de responsabilidades administrativas.

- c) Identificar a la persona ante quien se desarrolla la diligencia de auditoria.
- d) El registro de quejas y denuncias, que se formulen (por escrito o correo electrónico), así como en las investigaciones de las quejas y denuncias que se formulen en contra de servidores públicos de la administración pública estatal.
- e) Expedientes electrónicos personales de los servidores públicos, se resguardarán en el Sistema DeclaraNet Sinaloa.
- f) Recepción de solicitudes de información de datos personales presencial en nuestras oficinas.
- g) Realizar el registro de los participantes en las acciones de capacitación, validar la asistencia a los cursos, brindar la capacitación, generar las constancias respectivas, elaborar informes, en su caso, establecer comunicación para dar seguimiento a la conclusión de los cursos, así como para aclarar dudas sobre sus datos, ya sea por algún error o imprecisión, notificación de cancelación o cambio de horario, fecha y/o sede.
- h) En Programas Sociales, para el registro de asistencia a los distintos eventos y capacitaciones a realizarse, para la comprobación y evidencia, mismos que se dan de alta en el Sistema de Información de Contraloría Social (SICS), operado por la Secretaría de la Función Pública.

Para las finalidades antes señaladas y dependiendo de los datos personales a tratar, se recaban los siguientes datos:

- 1) Nombre completo.
- 2) Datos Laborales (nombre de la institución, sector al que pertenece, puesto, área de adscripción, correo electrónico y teléfono de oficina).
- 3) Edad.
- 4) Domicilio.

- 5) Nivel de escolaridad.
- 6) Referencias Personales, así como nombre de cónyuge, nombre del padre, nombre de la madre y datos personales de sus dependientes económicos.
- 7) Institución bancaria, número de cuenta y clabe interbancaria.

Adicional a lo anterior, se recaban los siguientes datos que se consideran sensibles: nombre de cónyuge y datos personales de sus dependientes económicos, certificado médico.

C. Derechos de los Titulares de los Datos Personales.

Para el ejercicio de cualquiera de los derechos Acceso, Rectificación, Cancelación y Oposición (ARCO) se deberá presentar la solicitud respectiva en la Dirección de Normatividad, con domicilio en Av. Lázaro Cárdenas #365, Colonia, Centro Sinaloa Culiacán, Sinaloa, C.P. 80000.

Para conocer el procedimiento y requisitos para el ejercicio de los derechos ARCO, se podrá llamar al siguiente número telefónico (667)716-32-53 Extensión 1007; o bien ponerse en contacto con nuestro Responsable de la Unidad de Transparencia, que dará trámite a las solicitudes para el ejercicio de estos derechos, y atenderá cualquier duda que se pudiera tener respecto al tratamiento de la información.

Los datos de contacto del Responsable de la Unidad de Transparencia son los siguientes Av. Lázaro Cárdenas # 365 , Colonia, Centro Sinaloa Culiacán, Sinaloa,C.P. 80000. .Teléfono (667)716-32-53 Extensión 1007 .

D. Área responsable de la implementación y observancia de esta política.

La Comisión Estatal de Agua Potable y Alcantarillado de Sinaloa, a través de la Dirección de Normatividad, tiene a su cargo la labor de desarrollo, implementación, capacitación y observancia de ésta Política. Para tal efecto, todos los servidores públicos que realizan el *Tratamiento de Datos Personales* en las diferentes áreas

de la Comisión, están obligados a reportar estas Bases de Datos y a dar traslado a ésta de manera inmediata, de todas las peticiones, quejas o reclamos que reciban por parte de los Titulares de Datos Personales.

El Comité de Transparencia será responsable de la atención de peticiones, consultas, quejas y reclamos ante la cual el titular de la información podrá ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización.

E. Autorización – Consentimiento.

El responsable deberá contar con el consentimiento previo del Titular para el tratamiento de los datos personales, el cual deberá otorgarse de forma:

- I. **Libre:** Sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular;
- II. **Específica:** Referida a finalidades concretas, lícitas, explícitas y legítimas que justifiquen el tratamiento; e
- III. **Informada:** Que el titular tenga conocimiento del aviso de privacidad previo al tratamiento a que serán sometidos sus datos personales.

En la obtención del consentimiento de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad declarada conforme a la ley, se estará a lo dispuesto en las reglas de representación previstas en la legislación civil que resulte aplicable.

El consentimiento podrá manifestarse de forma expresa o tácita:

- **Consentimiento expreso:** Es cuando la voluntad del titular se manifieste verbalmente, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología.

- **Consentimiento tácito:** Es cuando habiéndose puesto a disposición del titular el aviso de privacidad, éste no manifieste su voluntad en sentido contrario.

Por regla general será válido el consentimiento tácito, salvo que la ley o las disposiciones aplicables exijan que la voluntad del Titular se manifieste expresamente.

Tratándose de datos personales sensibles el responsable deberá obtener el consentimiento expreso y por escrito del Titular para su tratamiento, a través de su firma autógrafa, firma electrónica o cualquier mecanismo de autenticación que al efecto se establezca, salvo en los casos de excepción previstos en el artículo 22 de la LPDPPSOES.

Se considerará que el consentimiento expreso se otorgó por escrito cuando el titular lo externe mediante un documento con su firma autógrafa, huella dactilar o cualquier otro mecanismo autorizado por la normativa aplicable. En el entorno digital, podrán utilizarse medios como la firma electrónica o cualquier mecanismo o procedimiento equivalente que permita identificar fehacientemente al titular, y a su vez, recabar su consentimiento de tal manera que se acredite la obtención del mismo.

El responsable deberá informar al Titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.

F. Seguridad de los Datos Personales.

La CEAPAS, en estricta aplicación del *Principio de Seguridad en el Tratamiento de Datos Personales*, proporcionará las medidas técnicas, físicas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. La obligación y

responsabilidad de la CEAPAS, se limita a disponer de los medios adecuados para este fin.

La CEAPAS, no garantiza la seguridad total de su información ni se responsabiliza por cualquier consecuencia derivada de fallas técnicas o del ingreso indebido por parte de terceros a la Base de Datos o Archivo en los que reposan los Datos Personales objeto de Tratamiento por parte de la CEAPAS.

G. Tratamiento de Datos Personales.

La CEAPAS deberá darle un tratamiento a los datos personales recabados en estricto apego a los principios de Calidad, Confidencialidad, Consentimiento, Finalidad, Información, Lealtad y Legalidad en materia de tratamiento de datos personales, Licitud, Proporcionalidad, Responsabilidad y Seguridad, expresados en el Artículo 12 de la LPDPPSOES.

Se precisa que el servidor público que incumpla a los principios citados anteriormente será causa de sanción de acuerdo a lo dispuesto en el artículo 196 de LPDPPSOES.

H. Vigencia.

Esta Política de Protección de Datos Personales está vigente desde la fecha de su aprobación por el Comité de Transparencia de la CEAPAS.

V. Funciones y Obligaciones del personal involucrado en el tratamiento de datos personales.

Todos los servidores públicos que tengan acceso a los datos personales, están obligados a conocer y aplicar las medidas de seguridad propias que sean de carácter administrativo, físico y técnico para la protección de datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción, o en su caso, se deberá de garantizar la confidencialidad, integridad y disponibilidad.

Funciones genéricas en cualquier nivel de tratamiento:

- Tratar los datos personales con responsabilidad y las medidas de seguridad que se haya establecido para tal fin.

Obligaciones genéricas en cualquier nivel de tratamiento:

- Guardar confidencialidad sobre la información que se conozca en el desarrollo de sus actividades.
- Estar capacitado en materia de tratamiento de datos personales.
- Dar aviso a los superiores jerárquicos, ante cualquier acción que pueda poner en riesgo los datos personales, y en general que puedan vulnerar la seguridad de los datos personales.

El incumplimiento a lo establecido en este Documento de Seguridad, así como lo establecido por la LPDPPSOES, será causa de aplicación de medidas de apremio y/o sanción de acuerdo a lo dispuesto en el artículo 196 de LPDPPSOES.

VI. Inventarios de Datos Personales y de los Sistemas de Tratamiento

Los sistemas que se detallan en el presente documento son aquellos que contienen datos personales, que se encuentran tanto en soporte electrónico como físico.

Se presentan por Dirección y en orden con base al Reglamento Interior de la CEAPAS.

- A. Dirección Administrativa
- B. Dirección Normatividad
- C. Dirección de Licitaciones
- D. Dirección Técnica

En los siguientes apartados, se estará abordando cada uno de los sistemas señalando su descripción, estructura y medidas de seguridad. Dentro de este último se realizará un análisis de riesgos, el análisis de brecha y el plan de trabajo.

En la descripción de cada sistema de tratamiento de datos personales, se señala el fundamento legal, los datos personales que se encuentran en la dirección, la forma de obtención de los datos personales, el servidor público administrador del sistema, tipo de soporte, características del lugar físico donde se resguardan los datos personales, portabilidad de datos, transferencia de datos, encargado de datos.

Dirección Administrativa.

1.- Fundamento Legal.- Capitulo Seis, Sección IV Artículo 23 del Reglamento Interior de la Comisión Estatal de Agua Potable y Alcantarillado de Sinaloa.

2.-Datos Personales que se encuentran en esta Unidad Administrativa:



INVENTARIO DE DATOS PERSONALES GENERALES DIRECCION DE ADMINISTRACION

Marque con una **X** los datos personales que existen y son necesarios o que existen más no son necesarios en los procesos o trámites llevados a cabo en su Unidad Administrativa.

|

Datos Personales Recabados	Existente	Necesario	No necesario
Datos de identificación y contacto			
Nombre	X	X	
Alias			X
Seudónimo			X
Sexo	x	X	
Estado Civil	X	X	
Registro Federal de Contribuyentes (RFC)	X	X	
Registro Federal del instituto Nacional (INE)	X	X	
Clave Unica de Registro de Población (CURP)	X	X	
Lugar de Nacimiento	X	X	
Fecha de Nacimiento	X		X
Nacionalidad	X	X	
Domicilio	X	X	
Teléfono particular			X
Teléfono celular personal	X	X	
Correo electrónico personal	X	X	
Firma autógrafa	X	X	
Firma electrónica	x	x	
Edad	X		X
Fotografía	X	X	
Referencias personales	X	X	
Escolaridad	X	X	
Número de seguridad social o análogo	x	x	
Datos sobre características físicas			
Color de piel	X		
Color de cabello	X		
Señas particulares	X		
Estatura	X		
Peso	X		
Cicatrices	X		
Tipo de sangre	X		
Datos biomédicos			

Datos Personales Recabados	Existente	Necesario	No necesario
Imagen de iris			X
Huella dactilar			X
Palma de la mano			X
ADN (Código genético)			X
Datos laborales			
Puesto o cargo que desempeña	x	X	
Domicilio del trabajo	x	X	
Correo electrónico institucional	x	X	
Teléfono institucional	x	X	
Referencia laborales	x	x	
Información generada durante los procedimientos de reclutamiento; selección y contratación	x	X	
Experiencia/Capacitación laboral	X	x	
Datos académicos			
Trayectoria educativa	x	X	
Títulos	X	x	
Cedula profesional	x	X	
Certificados	X	x	
Reconocimientos			X
Datos migratorios			
Entrada al país			X
Salida de país			X
Tiempo de permanencia en el país			X
Calidad migratoria			X
Derechos de residencia			X
Aseguramiento			X
Repatriación			X
Datos patrimoniales y/o financieros			
Bienes muebles			X
Bienes inmuebles			X
Información fiscal			X
Historial crediticio/Buró de crédito			X
Ingresos			X
Egresos			X
Cuentas bancarias			X
Números de tarjetas de crédito			X
Información adicional de tarjeta (fechas de vencimiento, códigos de seguridad, datos de banda magnética, pin)			X
Seguros			X
Afores			X

Datos sobre pasatiempos, entretenimientos y diversión			
Datos Personales Recabados	Existente	Necesario	No necesario
Pasatiempos			X
Aficiones			X
Deportes de práctica			X
Juegos de su interés			X
Datos legales			
Situación jurídica de la persona (juicios, amparos, procesos administrativos, entre otros)		X	
Otros datos personales (mencionar)			



**INVENTARIO DE DATOS PERSONALES SENSIBLES
DIRECCION DE ADMINISTRACION**

Marque con una **X** los datos personales que existen y son necesarios o que existen más no son necesarios en los procesos o trámites llevados a cabo en su Unidad Administrativa.

Datos personales recabados	Existente	Necesario	No necesario
Datos de identificación y contacto			
Posturas religiosas/ ideológicas/morales/filosóficas			X
Pertenencia a un partido/Posturas políticas			X
Pertenencia a un sindicato		X	
Datos de Salud			
Estado de salud físico presente, pasado o futuro	X		
Estado de salud mental presente, pasado o futuro			X
Información genética			X
Datos sobre vida sexual			
Preferencias sexuales			X
Prácticas o hábitos sexuales			X
Datos de origen étnicos o racial			
Pertenencia a un pueblo, etnia o región			X
Datos Familiares			
Relaciones afectivas, familiares y conyugales			x
Otros datos personales (mencionar)			

3.- Forma de obtención de los datos personales. - se obtienen mediante un formulario físico.

4.- Servidor Público Administrador de la Dirección:

Cargo: Directora Administrativo

Teléfono y Extensión: 6677163253 Ext 1012

Funciones/Perfil: Cumplir con las funciones que correspondan al puesto de conformidad con el Reglamento Interior de la CEAPAS, y realizar aquellas que le encomienden sus superiores jerárquicos.

Obligaciones: Entre otras, tramitar las designaciones del personal y creación de plazas en las unidades administrativas, realizar las gestiones requeridas para el pago de nóminas.

5.- Tipo de Soporte.- El soporte de los datos personales se encuentra el físico.

6.- Características del lugar donde se resguardan los sistemas de tratamiento de datos personales.- El área Administrativa de la CEAPAS se encuentra en Av. Lázaro Cárdenas #365, Centro Sinaloa, Culiacán, Sinaloa. Los archivos físicos se encuentran en una oficina con acceso restringido, están depositados en archiveros con llave.

7.- Portabilidad de datos.- El área Administrativo no cuenta con ningún formato estructurado para la portabilidad de datos.

8.- Transferencia de datos.- El área Administrativo no transfiere los datos personales.

9.- Encargado de datos.- Dirección Administrativa.

Dirección Normativa.

1.- Fundamento Legal.- Capitulo Seis, Sección V Artículo 25 del Reglamento Interior de la Comisión Estatal de Agua Potable y Alcantarillado de Sinaloa.

2.-Datos Personales que se encuentran en esta Dirección:



INVENTARIO DE DATOS PERSONALES GENERALES DIRECCION DE NORMATIVIDAD

Marque con una **X** los datos personales que existen y son necesarios o que existen más no son necesarios en los procesos o trámites llevados a cabo en su Unidad Administrativa.



Datos Personales Recabados	Existente	Necesario	No necesario
Datos de identificación y contacto			
Nombre	X	X	
Alias			X
Seudónimo			X
Sexo			X
Estado Civil			X
Registro Federal de Contribuyentes (RFC)			X
Registro Federal del instituto Nacional (INE)			X
Clave Unica de Registro de Población (CURP)			X
Lugar de Nacimiento			X
Fecha de Nacimiento			X
Nacionalidad	X	X	
Domicilio			X
Teléfono particular		X	
Teléfono celular personal	X	X	
Correo electrónico personal	X	X	
Firma autógrafa			X
Firma electrónica			X
Edad			X
Fotografía			X
Referencias personales			X
Escolaridad			X
Número de seguridad social o análogo			X
Datos sobre características físicas			
Color de piel			X
Color de cabello			X
Señas particulares			X
Estatura			X
Peso			X
Cicatrices			X
Tipo de sangre			X
Datos biomédicos			

Datos Personales Recabados	Existente	Necesario	No necesario
Imagen de iris			X
Huella dactilar			X
Palma de la mano			X
ADN (Código genético)			X
Datos laborales			
Puesto o cargo que desempeña			X
Domicilio del trabajo			X
Correo electrónico institucional			X
Teléfono institucional			X
Referencia laborales			X
Información generada durante los procedimientos de reclutamiento; selección y contratación			X
Experiencia/Capacitación laboral			
Datos académicos			
Trayectoria educativa			X
Títulos			X
Cedula profesional			X
Certificados			X
Reconocimientos			X
Datos migratorios			
Entrada al país			X
Salida de país			X
Tiempo de permanencia en el país			X
Calidad migratoria			X
Derechos de residencia			X
Aseguramiento			X
Repatriación			X
Datos patrimoniales y/o financieros			
Bienes muebles			X
Bienes inmuebles			X
Información fiscal			X
Historial crediticio/Buró de crédito			X
Ingresos			X
Egresos			X
Cuentas bancarias			X
Números de tarjetas de crédito			X
Información adicional de tarjeta (fechas de vencimiento, códigos de seguridad, datos de banda magnética, pin)			X
Seguros			X
Afores			X

Datos sobre pasatiempos, entretenimientos y diversión			
Datos Personales Recabados	Existente	Necesario	No necesario
Pasatiempos			X
Aficiones			X
Deportes de practica			X
Juegos de su interés			X
Datos legales			
Situación jurídica de la persona (juicios, amparos, procesos administrativos, entre otros)			X
Otros datos personales (mencionar)			

□



INVENTARIO DE DATOS PERSONALES SENSIBLES DIRECCION DE NORMATIVIDAD

Marque con una **X** los datos personales que existen y son necesarios o que existen más no son necesarios en los procesos o trámites llevados a cabo en su Unidad Administrativa.

Datos personales recabados	Existente	Necesario	No necesario
Datos de identificación y contacto			
Posturas religiosas/ ideológicas/morales/filosóficas			X
Pertenencia a un partido/Posturas políticas			X
Pertenencia a un sindicato			X
Datos de Salud			
Estado de salud físico presente, pasado o futuro			X
Estado de salud mental presente, pasado o futuro			X
Información genética			X
Datos sobre vida sexual			
Preferencias sexuales			X
Prácticas o hábitos sexuales			X
Datos de origen étnicos o racial			
Pertenencia a un pueblo, etnia o región			X
Datos Familiares			
Relaciones afectivas, familiares y conyugales			x
Otros datos personales (mencionar)			

3.- Forma de obtención de los datos personales.- se obtienen mediante un formulario físico.

4.- Servidor Público Administrador de la Dirección:

Cargo: Directora de Normatividad

Teléfono y Extensión: 6677163253 Ext

1014

Funciones/Perfil: Cumplir con las funciones que correspondan al puesto de conformidad con el Reglamento Interior de la CEAPAS, y realizar aquellas que le encomienden sus superiores jerárquicos.

Obligaciones: Entre otras, recibir las solicitudes de acceso a la información darle seguimiento con las áreas respectivas.

5.- Tipo de Soporte.- El soporte de los datos personales se encuentra el físico.

6.- Características del lugar donde se resguardan los sistemas de tratamiento de datos personales.- El área de Normatividad de la CEAPAS se encuentra Av. Lázaro Cárdenas #365, Centro Sinaloa, Culiacán, Sinaloa. Los archivos físicos se encuentran en una oficina con acceso restringido, están depositados en archiveros.

7.- Portabilidad de datos.- El área Normativo no cuenta con ningún formato estructurado para la portabilidad de datos.

8.- Transferencia de datos.- El área Normativo no transfiere los datos personales.

9.- Encargado de datos.- Dirección de Normatividad.

Dirección Técnica.

1.- Fundamento Legal.- Capitulo Seis, Sección III Artículo 25 del Reglamento Interior de la Comisión Estatal de Agua Potable y Alcantarillado de Sinaloa.

2.-Datos Personales que se encuentran en esta Dirección:



INVENTARIO DE DATOS PERSONALES GENERALES DIRECCION DE TECNICA

Marque con una **X** los datos personales que existen y son necesarios o que existen más no son necesarios en los procesos o trámites llevados a cabo en su Unidad Administrativa.



Datos Personales Recabados	Existente	Necesario	No necesario
Datos de identificación y contacto			
Nombre	X	X	
Alias			X
Seudónimo			X
Sexo			X
Estado Civil			X
Registro Federal de Contribuyentes (RFC)	X	X	
Registro Federal del instituto Nacional (INE)	X	X	
Clave Unica de Registro de Población (CURP)	X	X	
Lugar de Nacimiento			X
Fecha de Nacimiento			X
Nacionalidad	X	X	
Domicilio	X	X	
Teléfono particular	X	X	
Teléfono celular personal	X	X	
Correo electrónico personal	X	X	
Firma autógrafa	X	X	
Firma electrónica	X	X	
Edad			X
Fotografía		X	
Referencias personales			X
Escolaridad	X	X	
Número de seguridad social o análogo	X	X	
Datos sobre características físicas			
Color de piel			X
Color de cabello			X
Señas particulares			X
Estatura			X
Peso			X
Cicatrices			X
Tipo de sangre			x
Datos biomédicos			

Datos Personales Recabados	Existente	Necesario	No necesario
Imagen de iris			X
Huella dactilar			X
Palma de la mano			X
ADN (Código genético)			X
Datos laborales			
Puesto o cargo que desempeña			X
Domicilio del trabajo			X
Correo electrónico institucional			X
Teléfono institucional			X
Referencia laborales			X
Información generada durante los procedimientos de reclutamiento; selección y contratación			X
Experiencia/Capacitación laboral			
Datos académicos			
Trayectoria educativa			X
Títulos			X
Cedula profesional			X
Certificados			X
Reconocimientos			X
Datos migratorios			
Entrada al país			X
Salida de país			X
Tiempo de permanencia en el país			X
Calidad migratoria			X
Derechos de residencia			X
Aseguramiento			X
Repatriación			X
Datos patrimoniales y/o financieros			
Bienes muebles			X
Bienes inmuebles			X
Información fiscal			X
Historial crediticio/Buró de crédito			X
Ingresos			X
Egresos			X
Cuentas bancarias			X
Números de tarjetas de crédito			X
Información adicional de tarjeta (fechas de vencimiento, códigos de seguridad, datos de banda magnética, pin)			X
Seguros			X
Afores			X

Datos sobre pasatiempos, entretenimientos y diversión			
Datos Personales Recabados	Existente	Necesario	No necesario
Pasatiempos			X
Aficiones			X
Deportes de practica			X
Juegos de su interés			X
Datos legales			
Situación jurídica de la persona (juicios, amparos, procesos administrativos, entre otros)			x
Otros datos personales (mencionar)			

□



**INVENTARIO DE DATOS PERSONALES SENSIBLES
DIRECCION DE TECNICA**

Marque con una **X** los datos personales que existen y son necesarios o que existen más no son necesarios en los procesos o trámites llevados a cabo en su Unidad Administrativa.

Datos personales recabados	Existente	Necesario	No necesario
Datos de identificación y contacto			
Posturas religiosas/ideológicas/morales/filosóficas			X
Pertenencia a un partido/Posturas políticas			X
Pertenencia a un sindicato			X
Datos de Salud			
Estado de salud físico presente, pasado o futuro			X
Estado de salud mental presente, pasado o futuro			X
Información genética			X
Datos sobre vida sexual			
Preferencias sexuales			X
Prácticas o hábitos sexuales			X
Datos de origen étnicos o racial			
Pertenencia a un pueblo, etnia o región			X
Datos Familiares			
Relaciones afectivas, familiares y conyugales			x
Otros datos personales (mencionar)			

3.- Forma de obtención de los datos personales.- se obtienen mediante un formulario físico.

4.- Servidor Público Administrador de la Dirección:

Cargo: Director Técnico

Teléfono y Extensión: 6677163253 Ext 1015

Funciones/Perfil: Cumplir con las funciones que correspondan al puesto de conformidad con el Reglamento Interior de la CEAPAS, y realizar aquellas que le encomienden sus superiores jerárquicos.

Obligaciones: Entre otras, entre otras llevar a cabo la coordinación de la CEAPAS con las demás instituciones de gobierno relacionadas con el sector hídrico.

5.- Tipo de Soporte.- El soporte de los datos personales se encuentra el físico.

6.- Características del lugar donde se resguardan los sistemas de tratamiento de datos personales.- El área de Técnica de la CEAPAS se encuentra en Av. Lázaro Cárdenas #365, Centro Sinaloa, Culiacán, Sinaloa. Los archivos físicos se encuentran en una oficina con acceso restringido, están depositados en archiveros.

7.- Portabilidad de datos.- El área Técnico no cuenta con ningún formato estructurado para la portabilidad de datos.

8.- Transferencia de datos.- El área Técnico no transfiere los datos personales.

9.- Encargado de datos.- Dirección Técnica.

Dirección Licitaciones y Contratos.

1.- Fundamento Legal.- Capitulo Seis, Sección VII Artículo 25 del Reglamento Interior de la Comisión Estatal de Agua Potable y Alcantarillado de Sinaloa.

2.-Datos Personales que se encuentran en esta Dirección:



INVENTARIO DE DATOS PERSONALES GENERALES DIRECCION DE LICITACIONES Y CONTRATOS

Marque con una **X** los datos personales que existen y son necesarios o que existen más no son necesarios en los procesos o trámites llevados a cabo en su Unidad Administrativa.

Datos Personales Recabados	Existente	Necesario	No necesario
Datos de identificación y contacto			
Nombre	X	X	
Alias			X
Seudónimo			X
Sexo			X
Estado Civil			X
Registro Federal de Contribuyentes (RFC)	X	X	
Registro Federal del instituto Nacional (INE)	X	X	
Clave Unica de Registro de Población (CURP)	X	X	
Lugar de Nacimiento			X
Fecha de Nacimiento			X
Nacionalidad	X	X	
Domicilio	X	X	
Teléfono particular	X	X	
Teléfono celular personal	X	X	
Correo electrónico personal	X	X	
Firma autógrafa	X	X	
Firma electrónica	X	X	
Edad			X
Fotografía		X	
Referencias personales			X
Escolaridad	X	X	
Número de seguridad social o análogo	X	X	
Datos sobre características físicas			
Color de piel			X
Color de cabello			X
Señas particulares			X
Estatura			X
Peso			X
Cicatrices			X
Tipo de sangre			x
Datos biomédicos			

Datos Personales Recabados	Existente	Necesario	No necesario
Imagen de iris			X
Huella dactilar			X
Palma de la mano			X
ADN (Código genético)			X
Datos laborales			
Puesto o cargo que desempeña			X
Domicilio del trabajo			X
Correo electrónico institucional			X
Teléfono institucional			X
Referencia laborales			x
Información generada durante los procedimientos de reclutamiento; selección y contratación			X
Experiencia/Capacitación laboral			
Datos académicos			
Trayectoria educativa			X
Títulos			X
Cedula profesional			X
Certificados			X
Reconocimientos			X
Datos migratorios			
Entrada al país			X
Salida de país			X
Tiempo de permanencia en el país			X
Calidad migratoria			X
Derechos de residencia			X
Aseguramiento			X
Repatriación			X
Datos patrimoniales y/o financieros			
Bienes muebles			X
Bienes inmuebles			X
Información fiscal			X
Historial crediticio/Buró de crédito			X
Ingresos			X
Egresos			X
Cuentas bancarias			X
Números de tarjetas de crédito			X
Información adicional de tarjeta (fechas de vencimiento, códigos de seguridad, datos de banda magnética, pin)			X
Seguros			X
Afores			X

Datos sobre pasatiempos, entretenimientos y diversión			
Datos Personales Recabados	Existente	Necesario	No necesario
Pasatiempos			X
Aficiones			X
Deportes de practica			X
Juegos de su interés			X
Datos legales			
Situación jurídica de la persona (juicios, amparos, procesos administrativos, entre otros)			x
Otros datos personales (mencionar)			



**INVENTARIO DE DATOS PERSONALES SENSIBLES
DIRECCION DE LICITACION Y CONTRATOS**

Marque con una **X** los datos personales que existen y son necesarios o que existen más no son necesarios en los procesos o trámites llevados a cabo en su Unidad Administrativa.

Datos personales recabados	Existente	Necesario	No necesario
Datos de identificación y contacto			
Posturas religiosas/ideológicas/morales/filosóficas			X
Pertenencia a un partido/Posturas políticas			X
Pertenencia a un sindicato			X
Datos de Salud			
Estado de salud físico presente, pasado o futuro			X
Estado de salud mental presente, pasado o futuro			X
Información genética			X
Datos sobre vida sexual			
Preferencias sexuales			X
Prácticas o hábitos sexuales			X
Datos de origen étnicos o racial			
Pertenencia a un pueblo, etnia o región			X
Datos Familiares			
Relaciones afectivas, familiares y conyugales			x
Otros datos personales (mencionar)			

3.- Forma de obtención de los datos personales.- se obtienen mediante un formulario físico.

4.- Servidor Público Administrador de la Dirección:

Cargo: Director Licitaciones y Contratos

Teléfono y Extensión: 6677163253

Funciones/Perfil: Cumplir con las funciones que correspondan al puesto de conformidad con el Reglamento Interior de la CEAPAS, y realizar aquellas que le encomienden sus superiores jerárquicos.

Obligaciones: Entre otras, entre otras vigilar que en el proceso de adjudicación y asignación de obras, bajo contrato se cumpla con las disposiciones legales y reglamentarias aplicables.

5.- Tipo de Soporte.- El soporte de los datos personales se encuentra el físico.

6.- Características del lugar donde se resguardan los sistemas de tratamiento de datos personales.- El área de Licitaciones y Contrato de la CEAPAS se encuentra en Av. Lázaro Cárdenas # 365, Centro Sinaloa, Culiacán, Sinaloa. Los archivos físicos se encuentran en una oficina con acceso restringido, están depositados en archiveros.

7.- Portabilidad de datos.- El área Licitaciones y Contratos no cuenta con ningún formato estructurado para la portabilidad de datos.

8.- Transferencia de datos.- El área Licitaciones y Contratos no transfiere los datos personales.

9.- Encargado de datos.- Dirección Licitaciones y Contratos.

VII. Medidas de Seguridad.

La LPDPPSOES, establece que se entenderá como medidas de seguridad al conjunto de acciones, actividades, controles o mecanismos administrativos, físicos y técnicos que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:

- I. Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión;
- II. Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales;
- III. Elaborar un inventario de datos personales y de los sistemas de tratamiento;
- IV. Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros;
- V. Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;

- VI.** Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales;
- VII.** Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales; y
- VIII.** Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

Derivado de lo anterior, el documento de seguridad debe contener al menos, el inventario de datos personales y de los sistemas de tratamiento, las funciones y obligaciones de las personas que traten datos personales, el análisis de riesgo, en análisis de brecha, el plan de trabajo, los mecanismos de monitoreo y revisión de las medidas de seguridad y el programa general de capacitación.

Las medidas de seguridad se abordaran en tres modalidades: Administrativas, Físicas y Técnicas.

Las Medidas de Seguridad Administrativas se traducen en políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales.

Las Medidas de Seguridad Físicas son el conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.

Las Medidas de Seguridad Técnicas son el conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento.

Como Medidas de Seguridad, de manera general, en la CEAPAS, cuenta con las siguientes:

De Tipo Físico:

- a) Prevenir el acceso no autorizado al perímetro de la CEAPAS, sus instalaciones físicas, áreas críticas, recursos e información;

Para lo anterior, la CEAPAS tiene personal en las entradas a las instalaciones, tiene por objeto la vigilancia, bienes y personas en las oficinas que ocupa la CEAPAS.

Tiene capacidad de respuesta inmediata y se ejecutan medidas de prevención, contención, neutralización y mitigación de los efectos adversos en el interior y la periferia de las oficinas, es decir, resguardan las instalaciones físicas, áreas críticas, recursos e información las 24 horas, los 365 días del año.

- b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la CEAPAS, recursos e información;

Se cuenta con normas, procedimientos y medidas de seguridad con el propósito de reducir al mínimo la incidencia de riesgos como: protocolo de acceso a las áreas estratégicas, protocolo ante sabotaje, protocolo de sismos y protocolo de incendios.

- c) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

Los equipos de cómputo de escritorio y portátiles que la CEAPAS asigna a los servidores públicos y áreas administrativas correspondientes para el cumplimiento de sus funciones, así como los equipos destinados al procesamiento, almacenamiento, transmisión y respaldo de la información relacionada a los Sistemas de Información, cuentan con mantenimiento periódico en el que se ejecutan acciones preventivas y en su caso, correctivas respaldadas por el personal de soporte técnico, con lo que se promueve un mantenimiento eficaz, disponibilidad de equipos y la información que hospedan.

De Tipo Técnico:

Se consideran aquellas medidas de seguridad aplicables en los sistemas de tratamiento de datos en soporte electrónico.

- a) Prevenir que el acceso a las bases de datos personales o a la información, así como a los recursos, sea por usuarios identificados y autorizados;
El acceso a la base de datos es exclusivo para el personal responsable del tratamiento de los datos personales de cada área. El acceso a las bases de datos se efectúa a través de Usuarios y Contraseñas asignado a cada operador de su equipo de cómputo.
- b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;

Las funciones del usuario de los sistemas de información, instituciones y de los responsables del tratamiento de datos personales en cada área, son definidas por las áreas responsables de los procesos respectivo.

- c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware.

La seguridad de todos los equipos de cómputo y de la red, está a cargo del personal de soporte técnico que cuenta con las herramientas tecnológicas para dicho fin con son firewall, antivirus, servicio de internet corporativo y restringido para los usuarios.

- d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

VIII. Análisis de Riesgos.

En el establecimiento de las medidas de seguridad, se debe considerar los riesgos existentes y la posibilidad de mitigarlos a través de un análisis cualitativo, sobre el impacto y la probabilidad de que se vulnere la seguridad, tanto en la información de datos personales como en los recursos involucrados. Este apartado se desarrolló tomando en cuenta:

- 1) Los requerimientos regulatorios, mejores prácticas de un sector específico.
- 2) El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida.
- 3) El valor y exposición de los activos involucrados en el tratamiento de los datos personales
- 4) Las consecuencias negativas para los titulares pudieran derivar de una vulneración de seguridad.
- 5) La sensibilidad de los datos personales tratados.
- 6) El desarrollo tecnológico.
- 7) Las posibles consecuencias de una vulneración para los titulares.
- 8) El número de titulares.
- 9) Las vulneraciones previas ocurridas.

Los factores pueden ser:	
Personas	Servidor público que se encuentra relacionado con el tratamiento y seguridad de los datos.
Procesos	Actividades y tareas necesarias para llevar a cabo el tratamiento de los datos.
Tecnología	Conjunto de Herramientas tecnológicas que intervienen de manera directa o indirecta en tratamiento y seguridad de los datos.
Infraestructura	Conjunto de recursos físicos que apoyan el funcionamiento de la organización y de manera específica el sistema de datos.

La clasificación pueden ser:	
TIC	Tecnologías de la información y comunicación. (Software y Hardware)
Capacitación	Desconocimiento de los Procesos.
Control	Falta de control.
Recursos	Humanos, financieros, materiales.

El control pueden ser:	
Interno	Si depende de la Dirección.
Externo	Si dependen de alguna otra Dirección.
Terceros	Si se refiere a algún ente externo a la CEAPAS.

Los valores pueden ser:		Valor	Semáforo	Nota
Impacto Alto =3	P. de O. Alto=3	9	Rojo	En caso de Datos personales sensibles, el impacto siempre será alto.
	P. de O. Medio=2	8	Rojo	
	P. de O. Bajo=1	7	Rojo	
Impacto Medio =2	P. de O. Alto=3	6	Naranja	
	P. de O. Medio=2	5	Naranja	
	P. de O. Bajo=1	4	Naranja	
Impacto Bajo =1	P. de O. Alto=3	3	Amarillo	
	P. de O. Medio=2	2	Amarillo	
	P. de O. Bajo=1	1	Amarillo	

IX. Análisis de Brecha.

En este apartado, se consideraron las medidas de seguridad existentes y los riesgos identificados, para determinar cuáles son las medidas de seguridad faltantes.

X. Plan de Trabajo.

Una vez realizado en análisis de riesgo y el análisis de brecha, cada dirección elaboro un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para su cumplimiento cotidiano de la política y tratamiento de los datos personales.

XI. Metodología para la redacción y vinculación de la información.

Para el desarrollo de las medidas de seguridad actuales, el análisis de riesgo, el análisis de brecha y el plan de trabajo, se manejan claves de identificación (ID) como una herramienta metodológica para realizar referencias y evitar la repetición en la escritura, ya que todos los subtemas están vinculados.

Los ID a utilizar en el documento de seguridad están integrados por 4 dígitos alfanuméricos:

Primer dígito: Empieza con una letra Mayúscula que corresponde a una Dirección de la CEAPAS.

Segundo dígito: Continúa con un número consecutivo del sistema de tratamiento de datos personales.

Tercer dígito: Se incorpora un número consecutivo, seguido de un punto, según el tema que se trate. Así, cuando se refieren las medidas de seguridad, se utiliza en número 1, para los riesgos o amenazas, se utiliza en número 2, al describir las brechas se utiliza en número 3 y la referencia del plan de trabajo, se hace con el número 4.

Cuarto dígito: Finalmente se integra por otro número consecutivo, del 1 al "x", que indica el número de la medida, el riesgo, la brecha o la actividad referida.

Dirección Administrativa.

1. Medidas de Seguridad actuales:

TIPO	CONTROL/MECANISMO	ID	MEDIDAS ACTUALES
ADMINISTRATIVAS	Políticas interna de protección de datos personales.	A1.1.1	El personal encargado del tratamiento de los datos personales tomo cursos de capacitación de las políticas asegurar, sobre sus deberes y sanciones en caso de no aplicarlos, administran los expedientes que contienen datos personales por orden alfabético.
	Conocimiento y cumplimiento de los deberes en el tratamiento de datos personales.		
	Conocimiento de las sanciones y medidas de apremio contempladas en la LPDPPSOES.		
	Proceso general de atención de derechos ARCO.		
FÍSICAS	Prevenir el Acceso no autorizado a la oficina donde se tienen resguardados los datos personales.	A2.1.1	La oficina donde se almacenan los expedientes con datos personales se encuentra con acceso restringido, los expedientes se encuentran en archiveros metálicos con llave para poder abrirlos, solo una persona tiene acceso a estos expedientes.
	Los expedientes deben de estar en archiveros con llave.	A2.1.2	
	No dejar expedientes sobre el escritorio si no se están utilizando.	A2.1.3	

2. Análisis de Riesgos:

Medidas de seguridad actuales	ID	Riesgo/amenaza	Factor de Riesgo	Clasificación del Riesgo	Control del Factor	Valoración de Riesgo	
						Impacto/probabilidad de que ocurra	valor
A1.1.1	A1.2.1	Cambio en el personal encargado del tratamiento de los datos personales.	Personas	Capacitación	Interno	3/P. de O.=1	7
A2.1.1	A2.2.1	Dejar la Puerta Abierta.	Personas	Control	Interno	2/P. de O.=1	4
A2.1.2	A2.2.2	Que se dañe el cerrojo de los archiveros y no existan recursos para repararlos y/o no se reporte el daño.	Infraestructura y/o Personas	Recursos	Interno	1/P. de O.=1	1
A2.1.3	A2.2.3	Que personal no autorizado se lleve el expediente.	Personas	Control	Interno	2/P. de O.=1	4

3. Análisis de Brecha:

Medidas de seguridad actuales	Riesgos	ID	Identificación de la Brecha
A1.1.1	A1.2.1	A1.3.1	Capacitación para nuevos ingresos.
A2.1.1	A2.2.1	A2.3.1	Asegurarse que la puerta se cierre cuando se ingrese a la oficina.
A2.1.2	A2.2.2	A2.3.2	Reportar la descompostura de inmediato
A2.1.3	A2.2.3	A2.3.3	Solo utilizar la información necesaria.

4.- Plan de Trabajo:

Brecha que se Atiende	Planificación			Evidencia/Entregable	
	ID	Actividad	Responsable		Fecha Tentativa
A1.3.1	A1.4.1	Solicitar capacitación cada que cambie personal encargado de la seguridad y tratamiento de los datos personales.	Dirección Administrativa	NA	Lista de asistencia a capacitación
A2.3.1	A2.4.1	Colocar letrero en la puerta de entrada al espacio de trabajo, donde recuerde cerrarla al entrar.	Dirección Administrativa	De inmediato	Fotografía
A2.3.2	A2.4.2	Llevar un control periódico del estado físico en que se encuentran los Archiveros.	Dirección Administrativa	Cada mes	Control Periódico
A2.3.3	A2.4.3	Poner letreros en la oficina donde se invite a sólo utilizar el expediente que se necesite y a archivarlo en cuanto se desocupe.	Dirección Administrativa	De inmediato	Fotografía

Dirección de Normatividad

1. Medidas de Seguridad actuales:

TIPO	CONTROL/MECANISMO	ID	MEDIDAS ACTUALES
ADMINISTRATIVAS	Políticas interna de protección de datos personales.	B1.1.1	El personal encargado del tratamiento de los datos personales tomo cursos de capacitación de las políticas asegurar, sobre sus deberes y sanciones en caso de no aplicarlos, administran los expedientes que contienen datos personales por número de denuncia.
	Conocimiento y cumplimiento de los deberes en el tratamiento de datos personales.		
	Conocimiento de las sanciones y medidas de apremio contempladas en la LPDPPSOES.		
	Proceso general de atención de derechos ARCO.		
FÍSICAS	Prevenir el Acceso no autorizado a la oficina donde se tienen resguardados los datos personales.	B2.1.1	La oficina donde se almacenan los expedientes con datos personales se encuentra con acceso restringido, cuenta personal que autoriza el ingreso, los expedientes se encuentran en archiveros metálicos con llave para poder abrirlos, el personal de la dirección tiene acceso a los expedientes,.
	Los expedientes deben de estar en archiveros con llave.	B2.1.2	
	No dejar expedientes sobre el escritorio si no se están utilizando.	B2.1.3	
TECNOLÓGICAS	Para ingresar al equipo de cómputo se necesita proporcionar usuario y contraseña.	B3.1.1	El equipo de cómputo donde se escanean las listas de asistencia se requiere un usuario y contraseña para su acceso, tiene antivirus y Fireworks que lo protegen.
	El equipo de cómputo se encuentra protegido con acceso, por antivirus y Fireworks.	B3.1.2	

2. Análisis de Riesgos:

Medidas de seguridad actuales	ID	Riesgo/amenaza	Factor de Riesgo	Clasificación del Riesgo	Control del Factor	Valoración de Riesgo	
						Impacto/probabilidades que ocurra	valor
B1.1.1	B1.2.1	Cambio en el personal encargado del tratamiento de los datos personales.	Personas	Capacitación	Interno	3/P. de O.=1	7
B2.1.1	B2.2.1	Dejar la Puerta Abierta.	Personas	Control	Interno	2/P. de O.=1	4
B2.1.2	B2.2.2	Que se descompongan el cerrojo de los archiveros y no existan recursos para repararlos.	Infraestructura	Recursos	Interno	1/P. de O.=1	1
B2.1.3	B2.2.3	Que personal no autorizado se lleve el expediente.	Personas	Control	Interno	2/P. de O.=1	4
B3.1.1	D3.2.1	Que se abandone el lugar y se deje la sesión abierta.	Personas	Control	Interno	2/P. de O.=1	4
B3.1.2	D3.2.2	Que en Fireworks y antivirus expire su licencia y quede desprotegido el equipo.	Tecnología	Recursos	Interno	2/P. de O.=1	4

3. Análisis de Brecha:

Medidas de seguridad actuales	Riesgos	ID	Identificación de la Brecha
B1.1.1	B1.2.1	B1.3.1	Capacitación para nuevos ingresos.
B2.1.1	B2.2.1	B2.3.1	Asegurarse que la puerta se cierre cuando se ingrese a la oficina.
B2.1.2	B2.2.2	B2.3.2	Reportar la descompostura de inmediato.
B2.1.3	B2.2.3	B2.3.3	Solo utilizar la información necesaria.
B3.1.1	B3.2.1	B3.3.1	Siempre cerrar sesión cuando se desocupe el equipo de cómputo.
B3.1.2	B3.2.2	B3.3.2	Siempre tener vigentes las licencias de antivirus y Fireworks.

4.- Plan de Trabajo:

Brecha que se Atiende	Planificación				Evidencia/Entregable
	ID	Actividad	Responsable	Fecha Tentativa	
B1.3.1	B1.4.1	Solicitar capacitación cada que cambie personal encargado de la seguridad y tratamiento de los datos personales	Dirección de Normatividad	NA	Lista de asistencia a capacitación
B2.3.1	B2.4.1	Poner Letrero en la puerta, donde recuerde cerrar la puerta al entrar	Dirección de Normatividad	De inmediato	Fotografía
B2.3.2	B2.4.2	Llevar un control periódico del estado físico en que se encuentran los Archiveros	Dirección de Normatividad	Cada mes	Control Periódico
B2.3.3	B2.4.3	Poner Letreros en la oficina donde se invite a solo utilizar el expediente que se necesite y a archivarlo en cuanto se desocupe	Dirección de Normatividad	De inmediato	Fotografía

B3.3.1	B3.4.1	Poner Letrero donde se recuerde cerrar sesión cada vez que se deje de utilizar el equipo de cómputo.	Dirección de Normatividad	De inmediato	Fotografía
B3.3.2	B3.4.2	Llevar control de las licencias y vigencias de los antivirus y Fireworks.	Dirección de Normatividad	De inmediato	Control Periódico

Dirección Técnica

1. Medidas de Seguridad actuales:

TIPO	CONTROL/MECANISMO	ID	MEDIDAS ACTUALES
ADMINISTRATIVAS	Políticas interna de protección de datos personales.	C1.1.1	El personal encargado del tratamiento de los datos personales tomo cursos de capacitación de las políticas asegurar, sobre sus deberes y sanciones en caso de no aplicarlos.
	Conocimiento y cumplimiento de los deberes en el tratamiento de datos personales.		
	Conocimiento de las sanciones y medidas de apremio contempladas en la LPDPPSOES.		
	Proceso general de atención de derechos ARCO.		
FÍSICAS	Prevenir el Acceso no autorizado a la oficina donde se tienen resguardados los datos personales.	C2.1.1	La oficina donde se almacenan los expedientes con datos personales se encuentra con acceso restringido, cuenta personal que autoriza el ingreso, los expedientes se encuentran en archiveros metálicos con llave para poder abrirlos, el personal de la dirección tiene acceso a los expedientes,.
	Los expedientes deben de estar en archiveros con llave.	C2.1.2	
	No dejar expedientes sobre el escritorio si no se están utilizando.	C2.1.3	

2. Análisis de Riesgos:

Medidas de seguridad actuales	ID	Riesgo/amenaza	Factor de Riesgo	Clasificación del Riesgo	Control del Factor	Valoración de Riesgo	
						Impacto/probabilidad de que ocurra	valor
C1.1.1	C1.2.1	Cambio en el personal encargado del tratamiento de los datos personales.	Personas	Capacitación	Interno	1/P. de O.=3	3
C2.1.1	C2.2.1	Dejar la Puerta Abierta.	Personas	Control	Interno	1/P. de O.=3	3
C2.1.2	C2.2.2	Que se descompongan el cerrojo de los archiveros y no existan recursos para repararlos.	Infraestructura	Recursos	Interno	1/P. de O.=1	1
C2.1.3	C2.2.3	Que personal no autorizado se lleve el expediente.	Personas	Control	Interno	1/P. de O.=1	1

3. Análisis de Brecha:

Medidas de seguridad actuales	Riesgos	ID	Identificación de la Brecha
C1.1.1	C1.2.1	C1.3.1	Capacitación para nuevos ingresos
C2.1.1	C2.2.1	C2.3.1	Asegurarse que la puerta se cierre cuando se ingrese a la oficina
C2.1.2	C2.2.2	C2.3.2	Reportar la descompostura de inmediato
C2.1.3	C2.2.3	C2.3.3	Solo utilizar la información necesaria

4.- Plan de Trabajo:

Brecha que se Atiende	Planificación				Evidencia/Entregable
	ID	Actividad	Responsable	Fecha Tentativa	
C1.3.1	C1.4.1	Solicitar capacitación cada que cambie personal encargado de la seguridad y tratamiento de los datos personales.	Dirección Técnica	NA	Lista de asistencia a capacitación
C2.3.1	C2.4.1	Poner Letrero en la puerta, donde recuerde cerrar la puerta al entrar.	Dirección Técnica	De inmediato	Fotografía
C2.3.2	C2.4.2	Llevar un control periódico del estado físico en que se encuentran los Archiveros.	Dirección Técnica	Cada mes	Control Periódico
C2.3.3	C2.4.3	Poner Letreros en la oficina donde se invite a solo utilizar el expediente que se necesite y a archivarlo en cuanto se desocupe.	Dirección Técnica	De inmediato	Fotografía

Dirección de Licitaciones y Contratos

1. Medidas de Seguridad actuales:

TIPO	CONTROL/MECANISMO	ID	MEDIDAS ACTUALES
ADMINISTRATIVAS	Políticas interna de protección de datos personales.	D1.1.1	El personal encargado del tratamiento de los datos personales tomo cursos de capacitación de las políticas a seguir, sobre sus deberes y sanciones en caso de no aplicarlos, administran los expedientes que contienen datos personales por fecha de la capacitación.
	Conocimiento y cumplimiento de los deberes en el tratamiento de datos personales.		
	Conocimiento de las sanciones y medidas de apremio contempladas en la LPDPPSOES.		
	Proceso general de atención de derechos ARCO.		
FÍSICAS	Prevenir el Acceso no autorizado a la oficina donde se tienen resguardados los datos personales.	D2.1.1	La oficina donde se almacenan los expedientes con datos personales se encuentra con acceso restringido, cuenta personal que autoriza el ingreso, los expedientes se encuentran en archiveros metálicos con llave para poder abrirlos, el personal de la dirección tiene acceso a los expedientes,.
	Los expedientes deben de estar en archiveros con llave.	D2.1.2	
	No dejar expedientes sobre el escritorio si no se están utilizando.	D2.1.3	

2. Análisis de Riesgos:

Medidas de seguridad actuales	ID	Riesgo/amenaza	Factor de Riesgo	Clasificación del Riesgo	Control del Factor	Valoración de Riesgo	
						Impacto/probabilidad de que ocurra	valor
D1.1.1	D1.2.1	Cambio en el personal encargado del tratamiento de los datos personales.	Personas	Capacitación	Interno	3/P. de O.=1	7
D2.1.1	D2.2.1	Dejar la Puerta Abierta.	Personas	Control	Interno	2/P. de O.=1	4
D2.1.2	D2.2.2	Que se descompongan el cerrojo de los archiveros y no existan recursos para repararlos.	Infraestructura	Recursos	Interno	1/P. de O.=1	1
D2.1.3	D2.2.3	Que personal no autorizado se lleve el expediente.	Personas	Control	Interno	2/P. de O.=1	4
D3.1.1	D3.2.1	Que se abandone el lugar y se deje la sesión abierta.	Personas	Control	Interno	2/P. de O.=1	4

3. Análisis de Brecha:

Medidas de seguridad actuales	Riesgos	ID	Identificación de la Brecha
D1.1.1	D1.2.1	D1.3.1	Capacitación para nuevos ingresos.
D2.1.1	D2.2.1	D2.3.1	Asegurarse que la puerta se cierre cuando se ingrese a la oficina.
D2.1.2	D2.2.2	D2.3.2	Reportar la descompostura de inmediato.
D2.1.3	D2.2.3	D2.3.3	Solo utilizar la información necesaria.

4.- Plan de Trabajo:

Brecha que se Atiende	Planificación				Evidencia/Entregable
	ID	Actividad	Responsable	Fecha Tentativa	
D1.3.1	D1.4.1	Solicitar capacitación cada que cambie personal encargado de la seguridad y tratamiento de los datos personales.	Dirección de Licitaciones y Contratos	NA	Lista de asistencia a capacitación
D2.3.1	D2.4.1	Poner Letrero en la puerta, donde recuerde cerrar la puerta al entrar.	Dirección de Licitaciones y Contratos	De inmediato	Fotografía
D2.3.2	D2.4.2	Llevar un control periódico del estado físico en que se encuentran los Archiveros.	Dirección de Licitaciones y Contratos	Cada mes	Control Periódico
D2.3.3	D2.4.3	Poner Letreros en la oficina donde se invite a solo utilizar el expediente que se necesite y a archivarlo en cuanto se desocupe.	Dirección de Licitaciones y Contratos	De inmediato	Fotografía
G3.3.1	G3.4.1	Poner Letrero donde se recuerde cerrar sesión cada vez que se deje de utilizar el equipo de cómputo.	Dirección de Auditoría	De inmediato	Fotografía
G3.3.2	G3.4.2	Llevar control de las licencias y vigencias de los antivirus y Fireworks.	Dirección de Auditoría	De inmediato	Control Periódico

XII. Mecanismos de Monitoreo.

En términos de lo dispuesto por la LPDPPSOES, para la protección de datos personales, la CEAPAS deberá establecer el monitoreo y revisión de manera periódica de las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que puedan estar sujetos los datos personales a su resguardo. Para ello y con base en el plan de trabajo planteado por cada dirección, se estará solicitando a cada Dirección envié a la Dirección de Normatividad, al Respetable de Transparencia, copia de la evidencia que sustente las actividades realizadas.

Posteriormente, en la actualización anual que corresponda, se estará trabajando con las titulares de cada dirección, respecto a la efectividad de las medidas de seguridad implementadas, con la finalidad de evitar alteración, pérdida o acceso no autorizado a los datos personales objeto de tratamiento.

XIII. Programa General de Capacitación.

Entre las atribuciones de la Dirección de Normatividad, está la de coordinar con la Dirección de Políticas de Transparencia, la capacitación continua y especializada del personal de la CEAPAS en materia de su competencia.

Derivado de lo anterior, la Dirección de Políticas de Transparencia junto con la CEAIP, capacita a todos los funcionarios públicos mediante el taller “Protección de Datos Personales, Medidas de Seguridad y Avisos de Privacidad”, particularmente se imparte este taller a todo nuevo servidor público que tenga entre sus actividades el tratamiento y resguardo de los datos personales.

XIV. Actualizaciones

De conformidad con lo establecido en el Artículo 47 de la LPDPPSOES, este documento de seguridad será actualizado cuando ocurra alguno de los siguientes eventos:

Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;

Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;

Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad;

Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

Así mismo como medida de actualización general, se establece que cuando se lleve a cabo la creación de un nuevo Aviso de Privacidad o Bases de Datos, el titular de la Dirección deberá dar aviso a la Dirección de Políticas de Transparencia de la creación del nuevo aviso o base de datos, con el objeto de integrarlos al inventario de datos personales.

Aprobación

El presente documento fue aprobado por unanimidad de los integrantes del Comité de Transparencia de la Comisión Estatal de Agua Potable y Alcantarillado del Estado de Sinaloa, en la Primera Sesión Extraordinaria efectuada el día 30 de Enero de 2025.