

DOCUMENTO DE SEGURIDAD

EN MATERIA DE TRATAMIENTO DE DATOS PERSONALES EN
POSESIÓN DEL INSTITUTO CATASTRAL DEL ESTADO DE SINALOA.

V.01

Contenido

I. Introducción.....	3
II. Marco Normativo.....	5
III. Ámbito de aplicación.....	6
IV. Política de Protección de Datos Personales del Instituto Catastral del Estado de Sinaloa.....	7
A. Responsable del Tratamiento de los Datos Personales y Fundamento para ello. 7	
B. Datos Sometidos a Tratamiento.....	7
C. Derechos de los Titulares de los Datos Personales.....	8
D. Área responsable de la implementación y observancia de esta política.....	9
E. Autorización – Consentimiento.....	9
F. Seguridad de los Datos Personales.....	11
G. Tratamiento de Datos Personales.....	11
V. Funciones y Obligaciones del personal involucrado en el tratamiento de datos personales.....	13
VI. Inventarios de Datos Personales y de los Sistemas de Tratamiento.....	14
Dirección de Servicios Informáticos.....	15
VII. Medidas de Seguridad.....	22
VIII. Análisis de Riesgos.....	27
IX. Análisis de Brecha.....	29
X. Plan de Trabajo.....	30
XI. Metodología para la redacción y vinculación de la información.....	31
Dirección de Servicios Informáticos.....	32
1. Medidas de Seguridad actuales:	32
2. Análisis de Riesgos:	32
3. Análisis de Brecha:	33
4.- Plan de Trabajo:.....	34
XII. Programa General de Capacitación.....	36
XIII. Actualizaciones.....	37
Aprobación.....	37

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, el Instituto Catastral del Estado de Sinaloa (ICES), 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, el ICES 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 Jurídica 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 (LGPDPESO).
- 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).
- 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 LPDPPSOES, el presente documento es aplicable para todas las áreas del ICES, 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, gráfica, alfanumérica, fotográfica, acústica o cualquier formato que haga identificable a una persona.

IV. Política de Protección de Datos Personales del Instituto Catastral del Estado de Sinaloa.

El ICES, 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 este Instituto, 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, el ICES es el 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.

B. Datos Sometidos a Tratamiento.

Los datos personales serán utilizados con la finalidad de:

- a) Avalúos en línea.
- b) Pagos en línea.

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

- 1) Nombre completo.
- 2) Clave de Registro de Peritos.
- 3) RFC.
- 4) Firma electrónica.
- 5) Correo electrónico.
- 6) Domicilio.
- 7) Clave Catastral.
- 8) Croquis de localización.
- 9) Fotos del inmueble.
- 10) Institución bancaria, número de cuenta.

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 el Instituto Catastral del Estado de Sinaloa, con domicilio en Miguel Tamayo Espinoza de los Monteros S/N Primer Piso, Colonia, Desarrollo Urbano Tres Ríos en Culiacán, Sinaloa, C.P. 80100.

Para conocer el procedimiento y requisitos para el ejercicio de los derechos ARCO, se podrá llamar al siguiente número telefónico (667)758-70-00 Extensión 3535; 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: Miguel Tamayo Espinoza de los Monteros S/N Primer Piso, Colonia,

Desarrollo Urbano Tres Ríos en Culiacán, Sinaloa, C.P. 80100.Teléfono (667)758-70-70 Extensión 3535.

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

El Instituto Catastral del Estado de Sinaloa, a través de la Dirección Jurídica, 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 del Instituto, 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.

El ICES, 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 del ICES, se limita a disponer de los medios adecuados para este fin.

El ICES, 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 del ICES.

G. Tratamiento de Datos Personales.

El ICES 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 del ICES.

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 con base al artículo 4, último párrafo y artículo 5 del Reglamento Interior de la Secretaría de Administración y Finanzas; así como los artículos relativos de la Ley de Catastro del Estado de Sinaloa.

A. Dirección de Servicios Informáticos

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 de Servicios Informáticos

1.- Fundamento Legal.- Se hace de su conocimiento que el fundamento para tratar sus datos personales, se encuentra en los artículos 21, 94, 165 y el segundo párrafo del artículo 166 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Sinaloa 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 Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Sinaloa y los demás relativos al Reglamento Interior de la Secretaria de Administración y finanzas.

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



DIRECCIÓN DE SERVICIOS INFORMÁTICOS

INVENTARIO DE DATOS PERSONALES GENERALES
PERSONAL DEL ICES

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 Única 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	X	
Teléfono celular personal	X	X	
Correo electrónico personal			X
Firma autógrafa			X
Firma electrónica	X	X	
Edad	X	X	
Fotografía			X
Referencias personales			X
Escolaridad	X	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	X	
Domicilio del trabajo			
Correo electrónico institucional	X	X	
Teléfono institucional			X
Referencia laborales			X
Información generada durante los procedimientos de reclutamiento; selección y contratación	X		
Experiencia/Capacitación laboral	X		
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	X	
Bienes inmuebles	X	X	
Información fiscal			X
Historial crediticio/Buró de crédito			X
Ingresos	X	X	
Egresos	X	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

2

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)			

Area: Dirección de Servicios Informáticos.



DIRECCIÓN DE SERVICIOS INFORMÁTICOS

INVENTARIO DE DATOS PERSONALES SENSIBLES
PERSONAL DEL ICES

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			
Datos de Salud			
Estado de salud físico presente, pasado o futuro			X
Estado de salud mental presente, pasado o futuro			
Información genética			X
Datos sobre vida sexual			
Preferencias sexuales			X
Prácticas o hábitos sexuales			
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)			

Area: Dirección de Servicios Informáticos.

DIRECCIÓN DE SERVICIOS INFORMÁTICOS



INVENTARIO DE DATOS PERSONALES GENERALES
PROPIETARIA/O, POSESIONARIA/O O AUTORIZADA LEGALMENTE

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
Clave Única de Registro de Población (CURP)			X
Lugar de Nacimiento		X	
Fecha de Nacimiento			X
Nacionalidad			X
Domicilio	X	X	
Teléfono particular	X	X	
Teléfono celular personal			X
Correo electrónico personal	X	X	
Firma autógrafa			X
Firma electrónica	X	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			X
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

2

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)			

Area: Dirección de Servicios Informáticos



DIRECCIÓN DE SERVICIOS INFORMÁTICOS

INVENTARIO DE DATOS PERSONALES SENSIBLES
PROPIETARIA/O, POSESIONARIA/O O AUTORIZADA LEGALMENTE

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			
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)			

Area: Dirección de Servicios Informáticos.

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

4.- Servidor Público Administrador de la Dirección:

Cargo: Director de Servicios Informáticos

Teléfono y Extensión: 667 758-7000 Ext 1591

5.- Tipo de Soporte.- El soporte de los datos personales se encuentra en electrónico.

6.- Características del lugar donde se resguardan los sistemas de tratamiento de datos personales.- La Dirección de Servicios Informáticos se encuentra en Calle Miguel Tamayo Espinoza de los monteros s/n 1er piso, Desarrollo Urbano Tres Ríos, Culiacán, Sinaloa. Los archivos electrónicos se encuentran en un servidor con acceso restringido, solo se puede ingresar mediante clave de acceso.

7.- Portabilidad de datos.- La Dirección de Servicios Informáticos cuenta con ningún formato estructurado para la portabilidad de datos.

8.- Transferencia de datos.- La Dirección de Servicios Informáticos no transfiere los datos personales.

9.- Encargado de datos.- Dirección de Servicios Informáticos.

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 el ICES cuenta con las siguientes:

De Tipo Físico:

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

Para lo anterior, el ICES se encuentra dentro de las instalaciones de la Unidad de Servicios Estatales (USE), la cual cuenta con personal de vigilancia que tiene por objeto la vigilancia, protección a instalaciones, bienes y personas en las oficinas que ocupa el ICES.

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 del ICES, 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 socio-organizativos (manifestaciones), protocolos de amenaza de bomba, protocolo de sismos y protocolo de incendios.

- c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización; y

En el ICES se cuenta con acciones y mecanismos que permiten proteger e identificar los equipos móviles y portátiles; mobiliario, documentos y materiales mediante controles de acceso al edificios tanto de entrada y salida, como son: control en el uso de aparatos electrónicos y eléctricos, control en el ingreso y egreso de aparatos, equipos, mobiliario, documentos y materiales previa autorización del Director de Área.

- d) 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 el ICES 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 interna de gobierno, está a cargo del personal de soporte técnico que cuenta con las herramientas tecnológicas para dicho fin con son Fireworks, 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 STRC.

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, la dirección elaboró 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 del ICES.

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 riegos 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 de Servicios Informáticos.

1. Medidas de Seguridad actuales:

TIPO	CONTROL/MECANISMO	ID	MEDIDAS ACTUALES
ADMINISTRATIVAS	Políticas interna de protección de datos personales.	A1.1.1	
	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.		
FISICAS	Prevenir el Acceso no autorizado a la oficina donde se tienen resguardados los datos personales.	A2.1.1	
	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	
TECNOLÓGICAS	Para ingresar al equipo de cómputo se necesita proporcionar usuario y contraseña.	A3.1.1	
	El equipo de cómputo se encuentra protegido con acceso restringido a la red de gobierno, por antivirus y Firewalls.	A3.1.2	

2. Análisis de Riesgos:

Medidas de seguridad actuales	ID	Riesgo/amenaza	Factor de Riesgo	Clasificación del Riesgo	Control del Factor	Valoración de Riesgo	
						Impacto/probabilidad de que ocurra	valor
A1.1.1	A1.2.1						
A2.1.1	A2.2.1						
A2.1.2	A2.2.2						
A2.1.3	A2.2.3						

3. Análisis de Brecha:

Medidas de seguridad actuales	Riesgos	ID	Identificación de la Brecha
A1.1.1	A1.2.1	A1.3.1	
A2.1.1	A2.2.1	A2.3.1	
A2.1.2	A2.2.2	A2.3.2	
A2.1.3	A2.2.3	A2.3.3	

4.- Plan de Trabajo:

Brecha que se Atiende	Planificación				Evidencia/Entregable
	ID	Actividad	Responsable	Fecha Tentativa	
A1.3.1	A1.4.1				
A2.3.1	A2.4.1				
A2.3.2	A2.4.2				
A2.3.3	A2.4.3				

Mecanismos de Monitoreo.

En términos de lo dispuesto por la LPDPPSOES, para la protección de datos personales, el ICES 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 envíe a la Dirección Jurídica, 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.

XII. Programa General de Capacitación.

Entre las atribuciones de la Unidad de Transparencia del ICES, está la de coordinar la capacitación continua y especializada del personal del ICES en materia de su competencia.

Derivado de lo anterior, la Unidad de Transparencia del ICES en coordinación Dirección de Políticas de Transparencia, solicita la capacitación para todos los funcionarios públicos referente al 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.

XIII. 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.

Estas modificaciones se realizarán y efectuarán, previa solicitud a la Dirección Jurídica, por parte de las unidades administrativas responsables de la protección de los datos personales.

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 Jurídica 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 del Instituto Catastral del Estado de Sinaloa, según consta en el Acta de Sesión Ordinaria 001-CT-ICES-2021, efectuada el día 22 de enero de 2021.



SINALOA
SECRETARÍA
DE ADMINISTRACIÓN
Y FINANZAS
INSTITUTO CATASTRAL
DEL ESTADO DE SINALOA

Unidad de Servicios
Estatales (USE)
Segundo piso
Desarrollo Urbano tres
Ríos, C.P. 80100
Culiacán, Sinaloa. México.

**COMITÉ DE TRANSPARENCIA DEL INSTITUTO
CATASTRAL DEL ESTADO DE SINALOA
ACTA DE SESION NUMERO: 001-CT-ICES-2021**

**ACTA DE SESIÓN DEL COMITÉ DE TRANSPARENCIA DEL INSTITUTO
CATASTRAL DEL ESTADO DE SINALOA PARA RATIFICAR EL DOCUMENTO
DE SEGURIDAD DE ESTE INSTITUTO**

En la ciudad de Culiacán, Sinaloa, siendo las doce horas con cinco minutos, del día viernes veintidós de enero del año dos mil veintiuno, se hace constar que el Comité de Transparencia del Instituto Catastral del Estado de Sinaloa se encuentra reunido en la Sala de Juntas del Instituto Catastral del Estado de Sinaloa, sito en la Unidad de Servicios Estatales (USE) ubicada en Boulevard Miguel Tamayo Espinoza de los Monteros, sin número, IV etapa, Desarrollo Urbano Tres Ríos, Culiacán Rosales, Sinaloa, para celebrar formal sesión del **Comité de Transparencia del Instituto Catastral del Estado de Sinaloa**, con el fin de analizar el asunto turnado por el Lic. Jesús Antonio Rojo Burgos responsable de la Unidad de Transparencia del Instituto Catastral del Estado de Sinaloa, con el propósito de que esta instancia revise y resuelva sobre la publicación del "Documento de Seguridad en Materia de Tratamiento de Datos Personales en posesión del Instituto Catastral del Estado de Sinaloa" y en atención a lo establecido por la fracción XVI del artículo 4, 45, 46, 47 y 111 de la Ley de Protección de Datos Personales en Posesión de sujetos obligados del Estado de Sinaloa, el señalado documento debe de ser aprobado y ratificado de forma anual por el Comité de Transparencia, al respecto, con fundamento en lo dispuesto por el artículo 66 fracción II en correlación con el numeral 141 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Sinaloa; en correlación al oficio SRTC/STCS/DPT/114/2021, signado por el Director de Políticas de Transparencia de la Secretaria de Transparencia y Rendición de Cuentas del Estado de Sinaloa, documento que se adjunta a esta acta, con el fin de otorgar respaldo a la presente sesión de

Carlos Menendez Gonzalez

Carlos Menendez Gonzalez

ratificación, se reúnen los miembros del **Comité de Transparencia del Instituto Catastral del Estado de Sinaloa** los C.C. Lic. Francisco Javier Vega Valles en su carácter de **Presidente del Comité de Transparencia**, Lic. Carlos Rene Conde González en su carácter de **Secretario Técnico del Comité de Transparencia**, y, Lic. Sandra Luz Guevara Cervantes, vocal del **Comité de Transparencia**.

Se procede a tomar en cuenta las siguientes:

CONSIDERACIONES

Que la Ley de Transparencia y Acceso a la Información Pública del Estado de Sinaloa, establece en su capítulo II, que el Comité de Transparencia, es el órgano colegiado que se integrará en cada uno de los sujetos obligados, por disposición expresa de la Ley de Transparencia y Acceso a la Información Pública del Estado de Sinaloa, el cual deberá conformarse por un número impar de servidores públicos y, en su caso, de personas designadas por su Titular, y que tendrá **facultades para confirmar, modificar o revocar** las determinaciones que en materia de ampliación del plazo de respuesta, **clasificación de la información** y declaración de inexistencia o de incompetencia, realicen los titulares de las áreas de los sujetos obligados.

El Comité de Transparencia en su calidad de órgano revisor, adoptará en forma colegiada sus resoluciones por unanimidad o mayoría de votos. En caso de empate el Presidente tendrá voto de calidad. Este acto deberá formalizarse mediante la elaboración del acta respectiva.

Con base en las consideraciones anteriores, y en atención al asunto descrito, el documento a ratificar aduce que el artículo 16 Constitucional incorpora a la lista de garantías fundamentales consagradas en nuestra carta magna, el derecho a la Protección 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 manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan en el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad, y salud públicas o para proteger los derechos de terceros.

Carlos Rene Conde Glaz. ST

Vega Valles

Se manifiesta que a partir de la publicación de la Ley de Protección de Datos Personales en Posesión de sujetos obligados del Estado de Sinaloa y los lineamientos de Protección de Datos Personales para sujetos obligados del Estado de Sinaloa, el Instituto Catastral del Estado de Sinaloa 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, garantizar los derechos de acceso, rectificación, cancelación y oposición de datos personales.

Que entre los deberes previstos en la Ley de Protección de Datos Personales en Posesión de sujetos obligados del Estado de Sinaloa, el Instituto Catastral del Estado de Sinaloa deberá de 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 dicho documento, para cumplir con lo que se establece en los artículos 35 de la Ley General de Protección de Datos Personales en Posesión de sujetos obligados y 42 de la Ley de Protección de Datos Personales local.

Que durante el desarrollo de la sesión fue leído y observado el documento de Seguridad en Materia de Tratamiento de Datos Personales en Posesión del Instituto Catastral del Estado de Sinaloa es procedente aprobarlo en su totalidad.

Que este Comité de Transparencia como órgano colegiado, en uso de las funciones establecidas en el artículo 111, fracciones I y II de la Ley de Protección de Datos Personales en Posesión de sujetos obligados del Estado de Sinaloa, por unanimidad resuelve emitir el siguiente:

ACUERDO

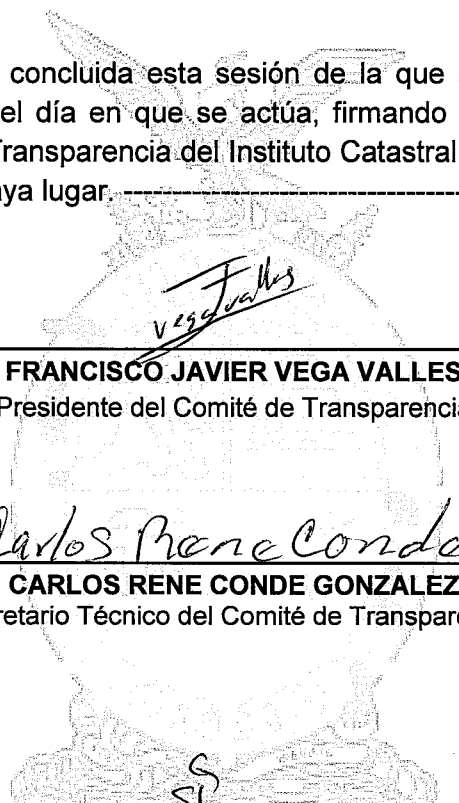
ÚNICO.- Se aprueba y se ratifica el Documento de Seguridad en Materia de Tratamiento de Datos Personales en posesión del Instituto Catastral del Estado de Sinaloa, así mismo, se instruye al Titular de Transparencia del Instituto Catastral del Estado de Sinaloa dar a conocer a los servidores públicos adscritos a este Instituto Catastral el documento aprobado y manifestarles la importancia de su observación y cumplimiento, lo anterior por la vía establecida en el mismo, en el apartado de difusión para acción.

Carlos Mena Conde 6/10/20



Lo anterior se resuelve por unanimidad de votos del Comité de Transparencia del Instituto Catastral del Estado de Sinaloa, con fundamento en el artículo 111, fracciones I y II de la Ley de Protección de Datos Personales en Posesión de sujetos obligados del Estado de Sinaloa, en la ciudad de Culiacán de Rosales, Sinaloa a los 22 días del mes de enero del año 2021.

Con lo anterior, se da por concluida esta sesión de la que se levanta la presente acta siendo las catorce horas del día en que se actúa, firmando al calce los intervinientes e integrantes del Comité de Transparencia del Instituto Catastral del Estado de Sinaloa, para los efectos legales a que haya lugar. -----



F. Vega Valles

FRANCISCO JAVIER VEGA VALLES

Presidente del Comité de Transparencia

Carlos Rene Conde Gonzalez

CARLOS RENE CONDE GONZALEZ

Secretario Técnico del Comité de Transparencia

S. L. Guevara Cervantes

SANDRA LUZ GUEVARA CERVANTES

Vocal del Comité de Transparencia

SINALOA