

DOCUMENTO DE SEGURIDAD

**[EN MATERIA DE TRATAMIENTO DE DATOS PERSONALES EN
POSESIÓN DEL INSTITUTO DE LA DEFENSORÍA PÚBLICA DEL
ESTADO DE SINALOA]**

Versión 1.0

Contenido

I.	Introducción.....	3
II.	Marco Normativo	4
III.	Ámbito de aplicación	4
IV.	Política de Protección de Datos Personales del Instituto de la Defensoría Pública.....	4
V.	Funciones y Obligaciones del personal involucrado en el tratamiento de datos personales.....	9
VI.	Inventarios de Datos Personales y de los Sistemas de Tratamiento	10
VII.	Medidas de Seguridad	34
VIII.	Análisis de Riesgos	35
IX.	Análisis de Brecha	37
X.	Plan de Trabajo	37
XI.	Metodología para la redacción y vinculación de la información	37
XII.	Mecanismos de Monitoreo	50
XIII.	Programa General de Capacitación	50
XIV.	Actualizaciones	50
	Aprobación.....	51

I. Introducción.

El 5 de julio de 2010 el Poder Ejecutivo Federal publicó en el Diario Oficial de la Federación la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

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 de la Defensoría Pública del Estado de Sinaloa (IDPES) 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 IDPES 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 del Instituto de la Defensoría Pública coordinó la elaboración de este documento.

Se elabora el presente Documento de seguridad de conformidad con lo establecido en el artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPSO) se establece la obligación del responsable de elaborar un documento de seguridad, así como ante lo establecido en el artículo 45 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Sinaloa.

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 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).
- Ley de la Defensoría Pública del Estado de Sinaloa (LDPES)
- Reglamento de la Ley de la Defensoría Pública del Estado de Sinaloa (RLDPES)
- Lineamientos de Protección de Datos Personales para Sujetos Obligados del Estado de Sinaloa.

III. Ámbito de aplicación.

El presente documento en atención a los "Deberes" que refiere la LPDPSOES es aplicable para todas las áreas del IDPES, 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 del Instituto de la Defensoría Pública.

El IDPES, 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 IDPES 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 11, 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) Expediente único de personal del IDP, a fin de realizar los trámites administrativos.
- b) Acciones de capacitación presencial dirigida a personal del IDP, para realizar el registro de los participantes en las acciones de capacitación dirigidas al personal del Instituto de la Defensoría Pública del Estado de Sinaloa, validar la asistencia a los cursos y para dar seguimiento a las capacitaciones, así como para la notificación de cancelación o cambio de horario, fecha y sede de las mismas.
- c) Servicios jurídicos en materia de Justicia para Adolescentes, a fin de generar registro y Base de Datos de las personas que solicitan los servicios jurídicos gratuitos. Para el inicio, continuidad y conclusión del procedimiento jurídico, para fines estadísticos e informes sobre el servicio brindado.
- d) Servicios jurídicos en materia Penal Segunda Instancia, a fin de generar registro y Base de Datos de las personas que solicitan los servicios jurídicos gratuitos. Para el inicio, continuidad y conclusión del procedimiento jurídico, para fines estadísticos e informes sobre el servicio brindado.
- e) Servicios jurídicos en materia Civil y Familiar, a fin de generar registro y Base de Datos de las personas que solicitan los servicios jurídicos gratuitos. Para el inicio, continuidad y conclusión del procedimiento jurídico, para fines estadísticos e informes sobre el servicio brindado.

- f) Servicios jurídicos en materia Penal Tradicional, a fin de generar registro y Base de Datos de las personas que solicitan los servicios jurídicos gratuitos. Para el inicio, continuidad y conclusión del procedimiento jurídico, para fines estadísticos e informes sobre el servicio brindado.
- g) Servicios jurídicos en materia Penal Sistema Acusatorio, a fin de generar registro y Base de Datos de las personas que solicitan los servicios jurídicos gratuitos. Para el inicio, continuidad y conclusión del procedimiento jurídico, para fines estadísticos e informes sobre el servicio brindado.
- h) Trámites ante la Unidad de Transparencia, con la finalidad de la admisión, trámite y respuesta de solicitudes de información interpuestas bajo la modalidad de datos personales, la información que se recabe en los recursos de revisión resultantes de inconformidades a las respuestas emitidas a los solicitantes, al dar trámite en los asuntos concernientes a los derechos ARCO.

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

- a) nombre
- b) edad
- c) sexo
- d) estado civil
- e) domicilio
- f) escolaridad
- g) nacionalidad
- h) número telefónico particular
- i) correo electrónico no oficial
- j) Registro Federal de Contribuyente
- k) CURP
- l) Datos académicos
- m) Datos laborales
- n) Estatus económico

De igual manera, se recaban los siguientes datos sensibles Estado de salud presente o futuro, Origen racial o étnico, Estado de salud física y mental, pasado, presente y futuro, Preferencias sexuales, Relaciones conyugales, Características físicas y Relaciones familiares.

C. Derechos de los Titulares de los Datos Personales.

Para ejercer los derechos de acceso, rectificación, cancelación u oposición de sus datos personales (derechos ARCO) se deberá presentar solicitud ante la Unidad de Transparencia del Instituto de la Defensoría Pública del Estado de Sinaloa, ubicada en domicilio Boulevard Rolando Arjona S/N, Colonia Juntas del Humaya, Culiacán, Sinaloa, C.P. 80050, teléfono (667)758-70-56, al correo elizabeth.rivas@sinaloa.gob.mx o bien a través de la Plataforma Nacional de Transparencia (<http://www.plataformadetransparencia.org.mx/>).

Si desea conocer el procedimiento para el ejercicio de estos derechos puede acudir a la Unidad de Transparencia del Instituto de la Defensoría Pública del Estado o bien enviar un correo electrónico a la dirección antes señalada.

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

La Dirección del Instituto de la Defensoría Pública, 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 IDPES, 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:

- a) **Libre:** Sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular;
- b) **Específica:** Referida a finalidades concretas, lícitas, explícitas y legítimas que justifiquen el tratamiento; e
- c) **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 IDPES, 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 IDPES, se limita a disponer de los medios adecuados para este fin.

El IDPES, no garantiza la seguridad total de su información ni se responsabiliza por cualquier consecuencia derivada de casos fortuitos, causas de fuerza mayor, 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 IDPES.

G. Tratamiento de Datos Personales.

El IDPES 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 STRC.

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 áreas y en orden con base al Reglamento Interior del IDPES.

- A. Dirección.
- B. Departamento del área penal
- C. Departamento del área civil y familiar
- D. Departamento especializado en justicia para adolescentes
- E. Departamento de formulación de agravios y amparo

F. Unidad de Transparencia

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

1.-Fundamento Legal: Capitulo II Artículo 29 de LDPES y Capitulo IX del Reglamento de la Ley de la Defensoría Pública del Estado de Sinaloa.

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

Esta Dirección cuenta con un aviso de privacidad para:

Expediente único de personal del IDP.

Acciones de capacitación presencial dirigida a personal del IDP



Instituto de la Defensoría Pública del Estado de Sinaloa Inventario de datos personales

Área: Dirección

Expediente único de personal del IDP

Seleccione con una "x" los datos personales que existen y son necesarios en los procesos o trámites de su área.

DATOS PERSONALES GENERALES		
Datos personales recabados	Existente	Necesario
Datos de identificación y contacto		
Nombre	X	X
Alias		
Seudónimo		
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	X
Teléfono Celular Personal	X	X
Correo electrónico personal	X	X
Firma autógrafa	X	X
Firma electrónica		
Edad	X	X
Fotografía		
Referencias Personales	X	X
Escolaridad	X	X
Número de seguridad social o análogo		
Datos sobre características físicas		
Color de piel	X	X
Color de cabello	X	X
Señas particulares	X	X
Estatura	X	X
Peso	X	X
Cicatrices	X	X
Tipo de sangre	X	X
Datos laborales		
Puesto o cargo que desempeña		
Área de adscripción		
Domicilio del trabajo		
Teléfono institucional		
Correo electrónico institucional		
Datos académicos		
Trayectoria educativa	X	X
Títulos	X	X
Cedula Profesional	X	X
Certificados		
Reconocimientos		
Datos patrimoniales o financieros		
Estatus económico		

DATOS PERSONALES SENSIBLES

Datos personales recabados

Existente

Necesario

Datos de identificación y contacto		
Posturas religiosas/ideológicas/morales/filosóficas		
Pertenencia a un partido/Posturas políticas		
Pertenencia a un sindicato		
Datos de salud		
Estado de salud físico presente, pasado y futuro.		
Estado de salud mental presente, pasado y futuro.		
Información genética		
Datos sobre vida sexual		
Preferencias sexuales		
Prácticas o hábitos sexuales		
Datos de origen étnicos o racial		
Pertenencia a un pueblo, etnia o región		
Datos familiares		
Relaciones afectivas, familiares y conyugales	X	X
Otras que mencionar		



Instituto de la Defensoría Pública del Estado de Sinaloa
Inventario de datos personales

Área: Dirección

Acciones de capacitación presencial dirigidas a personal del IDP

Seleccione con una "x" los datos personales que existen y son necesarios en los procesos o trámites de su área.

DATOS PERSONALES GENERALES		
Datos personales recabados	Existente	Necesario
Datos de identificación y contacto		
Nombre	X	X
Alias		
Seudónimo		

Sexo		
Estado Civil		
Registro Federal de Contribuyentes (RFC)		
Registro Federal del instituto Nacional (INE)		
Clave Unica de Registro de Población (CURP)		
Lugar de Nacimiento		
Fecha de Nacimiento		
Nacionalidad		
Domicilio		
Teléfono Particular	X	X
Teléfono Celular Personal		
Correo electrónico personal	X	X
Firma autógrafa	X	X
Firma electrónica		
Edad		
Fotografía		
Referencias Personales		
Escolaridad		
Número de seguridad social o análogo		
Datos sobre características físicas		
Color de piel		
Color de cabello		
Señas particulares		
Estatura		
Peso		
Cicatrices		
Tipo de sangre		
Datos laborales		
Puesto o cargo que desempeña	X	X
Área de adscripción	X	X
Domicilio del trabajo		
Teléfono institucional	X	X
Correo electrónico institucional	X	X
Datos académicos		
Trayectoria educativa		
Títulos		
Cedula Profesional		
Certificados		
Reconocimientos		
Datos patrimoniales o financieros		
Estatus económico		

DATOS PERSONALES SENSIBLES		
Datos personales recabados	Existente	Necesario
Datos de identificación y contacto		
Posturas religiosas/ideológicas/morales/filosóficas		
Pertenencia a un partido/Posturas políticas		
Pertenencia a un sindicato		
Datos de salud		
Estado de salud físico presente, pasado y futuro.		
Estado de salud mental presente, pasado y futuro.		
Información genética		
Datos sobre vida sexual		
Preferencias sexuales		
Prácticas o hábitos sexuales		
Datos de origen étnicos o racial		
Pertenencia a un pueblo, etnia o región		
Datos familiares		
Relaciones afectivas, familiares y conyugales		
Otras que mencionar		

3.-Forma de obtención de los datos personales: mediante un formato físico.

4.-Servidor Público Administrador de la Dirección:

Cargo: Director

Teléfono: 6677 178581

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

Obligaciones: Entre otras, Coordinar y supervisar las labores del personal a su cargo, administrar y coordinar la óptima utilización de los recursos humanos con que cuenta para el cumplimiento de sus objetivos;

5.- Tipo de Soporte: El soporte de los datos personales se encuentra el físico y de forma electrónica.

6.-Características del lugar donde se resguardan los sistemas de tratamiento de datos personales:

La Dirección del IDPES se encuentra en Blvd. Rolando Arjona S/N, Juntas del Humaya, Culiacán, Sinaloa. Los archivos físicos se encuentran en una oficina con acceso restringido, están depositados en archiveros con llave. Los archivos electrónicos se encuentran en una oficina la cual tiene acceso restringido, el equipo de cómputo del Administrador del sistema cuenta con clave y contraseña para poder acceder a él.

7.-Portabilidad de datos: La Dirección del IDPES no cuenta con ningún formato estructurado para la portabilidad de datos.

8.-Transferencia de datos: La Dirección del IDPES no transfiere los datos personales.

9.-Encargado de datos: Dirección.

Departamento del área penal

1.-Fundamento Legal: Capitulo XIII del Reglamento de la Ley de la Defensoría Pública del Estado de Sinaloa.

2.-Datos Personales que se encuentran en este Departamento:

Este Departamento cuenta con un aviso de privacidad para:

Servicios jurídicos en materia Penal Tradicional

Servicios jurídicos en materia Penal Sistema Acusatorio



**Instituto de la Defensoría Pública del Estado de Sinaloa
Inventario de datos personales**

Área: Departamento del área penal

Servicios jurídicos en materia penal tradicional

Seleccione con una "x" los datos personales que existen y son necesarios en los procesos o trámites de su área.

DATOS PERSONALES GENERALES		
Datos personales recabados	Existente	Necesario
Datos de identificación y contacto		
Nombre	X	X
Alias		
Seudónimo		
Sexo		
Estado Civil	X	X
Registro Federal de Contribuyentes (RFC)		
Registro Federal del instituto Nacional (INE)		
Clave Unica de Registro de Población (CURP)		
Lugar de Nacimiento		
Fecha de Nacimiento		
Nacionalidad		
Domicilio	X	X
Teléfono Particular	X	X
Teléfono Celular Personal		
Correo electrónico personal		
Firma autógrafa		
Firma electrónica		
Edad		
Fotografía		
Referencias Personales		
Escolaridad		
Número de seguridad social o análogo		
Datos sobre características físicas		
Color de piel		
Color de cabello		
Señas particulares		
Estatura		
Peso		
Cicatrices		
Tipo de sangre		
Datos laborales		
Puesto o cargo que desempeña		
Área de adscripción		
Domicilio del trabajo		
Teléfono institucional		
Correo electrónico institucional		
Datos académicos		
Trayectoria educativa		

Títulos		
Cedula Profesional		
Certificados		
Reconocimientos		
Datos patrimoniales o financieros		
Estatus económico		

DATOS PERSONALES SENSIBLES		
Datos personales recabados	Existente	Necesario
Datos de identificación y contacto		
Posturas religiosas/ideológicas/morales/filosóficas		
Pertenencia a un partido/Posturas políticas		
Pertenencia a un sindicato		
Datos de salud		
Estado de salud físico presente, pasado y futuro.	X	X
Estado de salud mental presente, pasado y futuro.	X	X
Información genética		
Datos sobre vida sexual		
Preferencias sexuales		
Prácticas o hábitos sexuales		
Datos de origen étnicos o racial		
Pertenencia a un pueblo, etnia o región		
Datos familiares		
Relaciones afectivas, familiares y conyugales		
Otras que mencionar		



Instituto de la Defensoría Pública del Estado de Sinaloa
Inventario de datos personales

Área: Departamento del área penal
Servicios jurídicos en materia penal Sistema Acusatorio

Seleccione con una "x" los datos personales que existen y son necesarios en los procesos o trámites de su área.

DATOS PERSONALES GENERALES		
Datos personales recabados	Existente	Necesario
Datos de identificación y contacto		
Nombre	X	X
Alias		
Seudónimo		
Sexo		
Estado Civil	X	X
Registro Federal de Contribuyentes (RFC)		
Registro Federal del instituto Nacional (INE)		
Clave Unica de Registro de Población (CURP)		
Lugar de Nacimiento		
Fecha de Nacimiento		
Nacionalidad		
Domicilio	X	X
Teléfono Particular	X	X
Teléfono Celular Personal		
Correo electrónico personal		
Firma autógrafa		
Firma electrónica		
Edad		
Fotografía		
Referencias Personales		
Escolaridad		
Número de seguridad social o análogo		
Datos sobre características físicas		
Color de piel		
Color de cabello		
Señas particulares		
Estatura		
Peso		
Cicatrices		
Tipo de sangre		
Datos laborales		
Puesto o cargo que desempeña		
Área de adscripción		
Domicilio del trabajo		
Teléfono institucional		
Correo electrónico institucional		

Datos académicos		
Trayectoria educativa		
Títulos		
Cedula Profesional		
Certificados		
Reconocimientos		
Datos patrimoniales o financieros		
Estatus económico		

DATOS PERSONALES SENSIBLES		
Datos personales recabados	Existente	Necesario
Datos de identificación y contacto		
Posturas religiosas/ideológicas/morales/filosóficas		
Pertenencia a un partido/Posturas políticas		
Pertenencia a un sindicato		
Datos de salud		
Estado de salud físico presente, pasado y futuro.	X	X
Estado de salud mental presente, pasado y futuro.	X	X
Información genética		
Datos sobre vida sexual		
Preferencias sexuales		
Prácticas o hábitos sexuales		
Datos de origen étnicos o racial		
Pertenencia a un pueblo, etnia o región		
Datos familiares		
Relaciones afectivas, familiares y conyugales		
Otras que mencionar		

3.-Forma de obtención de los datos personales: mediante registro físico.

4.-Servidor Público Administrador del Departamento:

Cargo: Jefe de Departamento del área penal

Teléfono: 6677 600409

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

Obligaciones: Entre otras, la coordinación de los asuntos que en esta materia atiende la Defensoría Pública, procurando su adecuada atención desde la etapa de averiguación previa o investigación hasta la ejecución de las penas, Organizar el Departamento a su cargo para la eficiente y eficaz prestación de los servicios en su área;

5.- Tipo de Soporte: El soporte de los datos personales se encuentra el físico y de forma electrónica.

6.-Características del lugar donde se resguardan los sistemas de tratamiento de datos personales: El Departamento del área penal se encuentra en Carretera a Navolato Km 9.5 S/N, Sindicatura de Aguaruto, Culiacán, Sinaloa. Los archivos físicos se encuentran en una oficina con acceso restringido, están depositados en archiveros con llave. Los archivos electrónicos se encuentran en una oficina la cual tiene acceso restringido, el equipo de cómputo del Administrador del sistema cuenta con clave y contraseña para poder acceder a él.

7.-Portabilidad de datos: El Departamento del área penal no cuenta con ningún formato estructurado para la portabilidad de datos.

8.-Transferencia de datos: El Departamento del área penal no transfiere los datos personales.

9.-Encargado de datos: Departamento del área penal.

Departamento del área civil y familiar

1.-Fundamento Legal: Capítulo XIII del Reglamento de la Ley de la Defensoría Pública del Estado de Sinaloa.

2.-Datos Personales que se encuentran en este Departamento:

Este Departamento cuenta con un aviso de privacidad para:
Servicios jurídicos en materia Civil y Familiar.



Instituto de la Defensoría Pública del Estado de Sinaloa
Inventario de datos personales

Área: Departamento del área Civil y Familiar
Servicios jurídicos en materia Civil y Familiar

Seleccione con una "x" los datos personales que existen y son necesarios en los procesos o trámites de su área.

DATOS PERSONALES GENERALES		
Datos personales recabados	Existente	Necesario
Datos de identificación y contacto		
Nombre	X	X
Alias		
Seudónimo		
Sexo	X	X
Estado Civil	X	X
Registro Federal de Contribuyentes (RFC)	X	X
Registro Federal del instituto Nacional (INE)		
Clave Unica de Registro de Población (CURP)		
Lugar de Nacimiento		
Fecha de Nacimiento		
Nacionalidad	X	X
Domicilio	X	X
Teléfono Particular	X	X
Teléfono Celular Personal		
Correo electrónico personal		
Firma autógrafa		
Firma electrónica		
Edad	X	X
Fotografía		
Referencias Personales		
Escolaridad		
Número de seguridad social o análogo	X	X
Datos sobre características físicas		
Color de piel		
Color de cabello		
Señas particulares		
Estatura		
Peso		

Cicatrices		
Tipo de sangre		
Datos laborales		
Puesto o cargo que desempeña		
Área de adscripción		
Domicilio del trabajo		
Teléfono institucional		
Correo electrónico institucional		
Datos académicos		
Trayectoria educativa		
Títulos		
Cedula Profesional		
Certificados		
Reconocimientos		
Datos patrimoniales o financieros		
Estatus económico	X	X

DATOS PERSONALES SENSIBLES		
Datos personales recabados	Existente	Necesario
Datos de identificación y contacto		
Posturas religiosas/ideológicas/morales/filosóficas		
Pertenencia a un partido/Posturas políticas		
Pertenencia a un sindicato		
Datos de salud		
Estado de salud físico presente, pasado y futuro.	X	X
Estado de salud mental presente, pasado y futuro.	X	X
Información genética		
Datos sobre vida sexual		
Preferencias sexuales	X	X
Prácticas o hábitos sexuales		
Datos de origen étnicos o racial		
Pertenencia a un pueblo, etnia o región	X	X
Datos familiares		
Relaciones afectivas, familiares y conyugales	X	X
Otras que mencionar		

3.-Forma de obtención de los datos personales: mediante formato físico.

4.-Servidor Público Administrador del Departamento:

Cargo: Jefe de Departamento del área civil y familiar

Teléfono: 6677 587325

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

Obligaciones: Entre otras, coordinará la prestación de los servicios del Instituto en los asuntos de esas materias, para su debida atención, Organizar el Departamento a su cargo para la eficiente y eficaz prestación de los servicios en su área;

5.- Tipo de Soporte: El soporte de los datos personales se encuentra el físico y de forma electrónica.

6.-Características del lugar donde se resguardan los sistemas de tratamiento de datos personales: El Departamento del civil y familiar se encuentra en Rolando Arjona S/N, Juntas del Humaya, Culiacán, Sinaloa. Los archivos físicos se encuentran en una oficina con acceso restringido, están depositados en archiveros con llave. Los archivos electrónicos se encuentran en una oficina la cual tiene acceso restringido, el equipo de cómputo del Administrador del sistema cuenta con clave y contraseña para poder acceder a él.

7.-Portabilidad de datos: El Departamento del área penal no cuenta con ningún formato estructurado para la portabilidad de datos.

8.-Transferencia de datos: El Departamento civil y familiar no transfiere los datos personales.

9.-Encargado de datos: Departamento del área civil y familiar.

Departamento especializado en justicia para adolescentes

1.-Fundamento Legal: Capitulo XIII del Reglamento de la Ley de la Defensoría Pública del Estado de Sinaloa.

2.-Datos Personales que se encuentran en este Departamento:

Este Departamento cuenta con un aviso de privacidad para:



Instituto de la Defensoría Pública del Estado de Sinaloa
Inventario de datos personales

Área: Departamento especializado en Justicia para Adolescentes
Servicios jurídicos en materia de Justicia para Adolescentes

Seleccione con una "x" los datos personales que existen y son necesarios en los procesos o trámites de su área.

DATOS PERSONALES GENERALES		
Datos personales recabados	Existente	Necesario
Datos de identificación y contacto		
Nombre	X	X
Alias		
Seudónimo		
Sexo		
Estado Civil		
Registro Federal de Contribuyentes (RFC)		
Registro Federal del instituto Nacional (INE)		
Clave Unica de Registro de Población (CURP)		
Lugar de Nacimiento		
Fecha de Nacimiento		
Nacionalidad		
Domicilio		
Teléfono Particular	X	X
Teléfono Celular Personal		
Correo electrónico personal		
Firma autógrafa		
Firma electrónica		
Edad	X	X
Fotografía		
Referencias Personales		
Escolaridad		
Número de seguridad social o análogo		
Datos sobre características físicas		
Color de piel		
Color de cabello		

Señas particulares		
Estatura		
Peso		
Cicatrices		
Tipo de sangre		
Datos laborales		
Puesto o cargo que desempeña		
Área de adscripción		
Domicilio del trabajo		
Teléfono institucional		
Correo electrónico institucional		
Datos académicos		
Trayectoria educativa		
Títulos		
Cedula Profesional		
Certificados		
Reconocimientos		
Datos patrimoniales o financieros		
Estatus económico		

DATOS PERSONALES SENSIBLES		
Datos personales recabados	Existente	Necesario
Datos de identificación y contacto		
Posturas religiosas/ideológicas/morales/filosóficas		
Pertenencia a un partido/Posturas políticas		
Pertenencia a un sindicato		
Datos de salud		
Estado de salud físico presente, pasado y futuro.	X	X
Estado de salud mental presente, pasado y futuro.	X	X
Información genética		
Datos sobre vida sexual		
Preferencias sexuales		
Prácticas o hábitos sexuales		
Datos de origen étnicos o racial		
Pertenencia a un pueblo, etnia o región		
Datos familiares		
Relaciones afectivas, familiares y conyugales		
Otras que mencionar		

3.-Forma de obtención de los datos personales: mediante registro físico.

4.-Servidor Público Administrador del Departamento:

Cargo: Jefe de Departamento especializado en justicia para adolescentes

Teléfono: 6677 609991

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

Obligaciones: Entre otras, coordinará la prestación del servicio de defensa ante autoridades, instituciones y órganos especializados en los procedimientos de justicia para adolescentes, Organizar el Departamento a su cargo para la eficiente y eficaz prestación de los servicios en su área;

5.- Tipo de Soporte: El soporte de los datos personales se encuentra el físico y de forma electrónica.

6.-Características del lugar donde se resguardan los sistemas de tratamiento de datos personales: El Departamento especializado en justicia para adolescentes se encuentra en Carretera a Navolato Km 9 S/N, Sindicatura de Aguaruto, Culiacán, Sinaloa. Los archivos físicos se encuentran en una oficina con acceso restringido, están depositados en archiveros con llave. Los archivos electrónicos se encuentran en una oficina la cual tiene acceso restringido, el equipo de cómputo del Administrador del sistema cuenta con clave y contraseña para poder acceder a él.

7.-Portabilidad de datos: El Departamento especializado en justicia para adolescentes no cuenta con ningún formato estructurado para la portabilidad de datos.

8.-Transferencia de datos: El Departamento especializado en justicia para adolescentes no transfiere los datos personales.

9.-Encargado de datos: Departamento especializado en justicia para adolescentes.

Departamento de formulación de agravios y amparo

1.-Fundamento Legal: Capitulo XIII del Reglamento de la Ley de la Defensoría Pública del Estado de Sinaloa.

2.-Datos Personales que se encuentran en este Departamento:

Este Departamento cuenta con un aviso de privacidad para:

Servicios jurídicos en materia Penal Segunda Instancia.



Instituto de la Defensoría Pública del Estado de Sinaloa
Inventario de datos personales

Área: Departamento especializado en formulación de Agravios y Amparo
Servicios jurídicos en materia penal Segunda Instancia

Seleccione con una "x" los datos personales que existen y son necesarios en los procesos o trámites de su área.

DATOS PERSONALES GENERALES		
Datos personales recabados	Existente	Necesario
Datos de identificación y contacto		
Nombre	X	X
Alias		
Seudónimo		
Sexo		
Estado Civil		
Registro Federal de Contribuyentes (RFC)		
Registro Federal del instituto Nacional (INE)		
Clave Unica de Registro de Población (CURP)		
Lugar de Nacimiento		
Fecha de Nacimiento		
Nacionalidad		
Domicilio		
Teléfono Particular	X	X
Teléfono Celular Personal		
Correo electrónico personal		
Firma autógrafa		
Firma electrónica		
Edad		
Fotografía		

Referencias Personales		
Escolaridad		
Número de seguridad social o análogo		
Datos sobre características físicas		
Color de piel		
Color de cabello		
Señas particulares		
Estatura		
Peso		
Cicatrices		
Tipo de sangre		
Datos laborales		
Puesto o cargo que desempeña		
Área de adscripción		
Domicilio del trabajo		
Teléfono institucional		
Correo electrónico institucional		
Datos académicos		
Trayectoria educativa		
Títulos		
Cedula Profesional		
Certificados		
Reconocimientos		
Datos patrimoniales o financieros		
Estatus económico		

DATOS PERSONALES SENSIBLES		
Datos personales recabados	Existente	Necesario
Datos de identificación y contacto		
Posturas religiosas/ideológicas/morales/filosóficas		
Pertenencia a un partido/Posturas políticas		
Pertenencia a un sindicato		
Datos de salud		
Estado de salud físico presente, pasado y futuro.		
Estado de salud mental presente, pasado y futuro.		
Información genética		
Datos sobre vida sexual		
Preferencias sexuales		
Prácticas o hábitos sexuales		

Datos de origen étnicos o racial		
Pertenencia a un pueblo, etnia o región		
Datos familiares		
Relaciones afectivas, familiares y conyugales		
Otras que mencionar		

3.-Forma de obtención de los datos personales: mediante registro físico.

4.-Servidor Público Administrador del Departamento:

Cargo: Jefe de Departamento de formulación de agravios y amparo

Teléfono: 6677 587000, extensión 39953

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

Obligaciones: Entre otras, coordinará la prestación del servicio relativo a la expresión de agravios en segunda instancia, ante el Supremo Tribunal de Justicia del Estado y las Salas de Circuito del Poder Judicial del Estado, y en su caso, lo relativo a demandas de amparo respecto a los asuntos en los que haya brindado representación el Instituto, así como la atención de los asuntos en materia Administrativa. Organizar el Departamento a su cargo para la eficiente y eficaz prestación de los servicios en su área;

5.- Tipo de Soporte: El soporte de los datos personales se encuentra el físico y de forma electrónica.

6.-Características del lugar donde se resguardan los sistemas de tratamiento de datos personales: El Departamento de formulación de agravios y amparo se encuentra en Rolando Arjona S/N, Juntas del Humaya, Culiacán, Sinaloa. Los archivos físicos se encuentran en una oficina con acceso restringido, están depositados en archiveros con llave. Los archivos electrónicos se encuentran en una oficina la cual tiene acceso restringido, el equipo de cómputo del Administrador del sistema cuenta con clave y contraseña para poder acceder a él.

7.-Portabilidad de datos: El Departamento de formulación de agravios y amparo no cuenta con ningún formato estructurado para la portabilidad de datos.

8.-Transferencia de datos: El Departamento de formulación de agravios y amparo no transfiere los datos personales.

9.-Encargado de datos: Departamento de formulación de agravios y amparo.

Unidad de Transparencia

1.-Fundamento Legal: Capitulo II Artículo 6 del Reglamento de la Ley de la Defensoría Pública del Estado de Sinaloa, Acuerdo que crea la Unidad de Transparencia del IDPES.

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

Esta Unida cuenta con avisos de privacidad para:

Trámites ante la Unidad de Transparencia.



Instituto de la Defensoría Pública del Estado de Sinaloa Inventario de datos personales

Área: Unidad de Transparencia

Tramites ante la Unidad de Transparencia

Seleccione con una "x" los datos personales que existen y son necesarios en los procesos o trámites de su área.

DATOS PERSONALES GENERALES		
Datos personales recabados	Existente	Necesario
Datos de identificación y contacto		
Nombre	X	X
Alias		
Seudónimo		
Sexo		
Estado Civil		
Registro Federal de Contribuyentes (RFC)		
Registro Federal del instituto Nacional (INE)		
Clave Unica de Registro de Población (CURP)		
Lugar de Nacimiento		
Fecha de Nacimiento		
Nacionalidad		
Domicilio		
Teléfono Particular		
Teléfono Celular Personal		
Correo electrónico personal	X	X
Firma autógrafa		

Firma electrónica		
Edad		
Fotografía		
Referencias Personales		
Escolaridad		
Número de seguridad social o análogo		
Datos sobre características físicas		
Color de piel		
Color de cabello		
Señas particulares		
Estatura		
Peso		
Cicatrices		
Tipo de sangre		
Datos laborales		
Puesto o cargo que desempeña		
Área de adscripción		
Domicilio del trabajo		
Teléfono institucional		
Correo electrónico institucional		
Datos académicos		
Trayectoria educativa		
Títulos		
Cedula Profesional		
Certificados		
Reconocimientos		
Datos patrimoniales o financieros		
Estatus económico		

DATOS PERSONALES SENSIBLES		
Datos personales recabados	Existente	Necesario
Datos de identificación y contacto		
Posturas religiosas/ideológicas/morales/filosóficas		
Pertenencia a un partido/Posturas políticas		
Pertenencia a un sindicato		
Datos de salud		
Estado de salud físico presente, pasado y futuro.		
Estado de salud mental presente, pasado y futuro.		
Información genética		

Datos sobre vida sexual		
Preferencias sexuales		
Practicas o hábitos sexuales		
Datos de origen étnicos o racial		
Pertenencia a un pueblo, etnia o región		
Datos familiares		
Relaciones afectivas, familiares y conyugales		
Otras que mencionar		

3.-Forma de obtención de los datos personales: mediante registro físico y de forma electrónica.

4.-Servidor Público Administrador del Departamento:

Cargo: Responsable de la Unidad de Transparencia del IDPES

Teléfono: 6677 587056

Funciones/Perfil: Cumplir con las funciones que correspondan al puesto de conformidad con el Reglamento de la LDPEs, el Acuerdo que crea la Unidad de Transparencia del IDPES, y realizar aquellas que le encomienden sus superiores jerárquicos.

Obligaciones: Entre otras, recabar y difundir la información a que se refieren las obligaciones de transparencia que le competan de conformidad con la Ley General y Estatal en materia de Transparencia y Datos Personales, recibir y dar trámite a las solicitudes de acceso a la información y datos personales.

5.- Tipo de Soporte: El soporte de los datos personales se encuentra el físico y de forma electrónica.

6.-Características del lugar donde se resguardan los sistemas de tratamiento de datos personales: la Unidad de Transparencia se encuentra en Blvd. Rolando Arjona S/N, Juntas del Humaya, Culiacán, Sinaloa. Los archivos físicos se encuentran en una oficina con acceso restringido, están depositados en archiveros con llave. Los archivos electrónicos se encuentran en una oficina la cual tiene acceso restringido, el equipo de cómputo del Administrador del sistema cuenta con clave y contraseña para poder acceder a él.

7.-Portabilidad de datos: La Unidad de Transparencia no cuenta con ningún formato estructurado para la portabilidad de datos.

8.-Transferencia de datos: La Unidad de Transparencia no transfiere los datos personales.

9.-Encargado de datos: Unidad de Transparencia del IDPES

VII. Medidas de Seguridad.

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.

Las áreas del IDPES reportaron de manera general las siguientes medidas de seguridad existentes:

- Quien recaba los datos personales, es un servidor público del área, asignado especialmente para recabar datos en general necesarios para cada trámite.
- El espacio físico o área donde se recaban datos personales, es dentro de las instalaciones.
- La mayoría de las oficinas cuenta con puertas que separa el área al momento de terminar labores.
- Las llaves que se tienen de cada área se encuentran en manos de servidores públicos, autorizados por cada área.
- Una vez recabados los datos personales, el servidor público genera un expediente físico y electrónico para cada trámite o servicio, del cual se obtuvieron los datos personales.

- Una vez recabados los datos personales, ya realizada la carpeta o expediente y guardada esta en archiveros o puesta en resguardo electrónico, tienen acceso a esta área servidores públicos del área.
- Una vez recabados los datos personales, en caso de que se les dé proceso electrónico, el servidor público autorizado guarda los mismos en carpeta electrónica en su computadora, carpeta compartida.
- Durante el desahogo del trámite del cual se obtuvieron los datos personales, los servidores públicos del área tienen acceso a los datos personales.
- Una vez concluido el trámite, los datos personales recabados se dejan intactos en la carpeta, archivo o expediente del trámite al que pertenecen.
- Cada carpeta de trámites o archivo, al terminar el proceso de cada uno, son resguardados en un archivo de cada área.

VIII. Análisis de Riesgos.

Debido a las circunstancias generales, tanto administrativas, físicas y técnicas, en las que se tratan datos personales, hemos logrado identificar los siguientes riesgos posibles ante los que se pudiera enfrentar el IDPES:

- Omitir la notificación al titular de los datos personales del aviso de privacidad.
- No difundir el aviso de privacidad.
- Ante la necesidad de tener un consentimiento expreso: no tener evidencia de que el titular de los datos personales conoce los términos del aviso de privacidad.
- Falta de capacitación de los servidores públicos en relación a la confidencialidad que deben guardar sobre los datos personales que conozcan debido al desempeño de sus funciones.
- No tener un lugar seguro y de acceso restringido en donde se puedan archivar los datos personales en físico.
- Permitir a todo servidor público o personas ajenas a la dependencia, el acceso a los expedientes que contienen datos personales.
- Pérdida de expedientes físicos debido a catástrofes, inundaciones, e incendios.
- Pérdida, robo o extravío de expedientes.
- Daño de la base de datos que contenga información confidencial.
- Fallas en los equipos de cómputo en donde se encuentran las bases de datos.

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: Herramientas tecnológicas que intervienen de manera directa o indirecta en tratamiento y seguridad de los datos.

Infraestructura: Recursos físicos que apoyan el funcionamiento de la organización y de manera específica el sistema de datos.

La clasificación puede 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 puede ser:

Interno: Cuando depende del área.

Externo: Cuando dependa de otra área.

Terceros: Cuando dependa de una dependencia externa al IDPES.

Los valores pueden ser:

Impacto	Probabilidad de ocurrencia	Valor	Semáforo	Observación
Alto=3	Alto=3 Medio=2 Bajo=1	9 8 7	Rojo Rojo Rojo	En Datos personales sensibles, el impacto siempre será alto.
Medio=2	Alto=3 Medio=2 Bajo=1	6 5 4	Amarillo Amarillo Amarillo	
Bajo=1	Alto=3 Medio=2 Bajo=1	3 2 1	Verde Verde Verde	

IX. Análisis de Brecha.

Se consideraron las medidas de seguridad existentes y los riesgos identificados, para determinar cuáles son las medidas de seguridad faltantes.

Las medidas de seguridad que actualmente se llevan a cabo pudieran ser efectivas de aplicarse de manera continua y consciente en las áreas del IDPES. El riesgo latente que se provoca por la falta de conocimiento, o compromiso para la aplicación de estas medidas existentes se puede minimizar por medio del establecimiento obligatorio de dichas medidas de seguridad y de la mejora continua de las mismas.

X. Plan de Trabajo.

La finalidad de este plan es plasmar de manera enunciativa, más no limitativa, las actividades que el IDPES realizará para la aplicación del presente documento de seguridad. Lo anterior se realizará en base a las atribuciones establecidas en la LPDPPSOES.

Para la elaboración de este plan de trabajo, primeramente se realizó el análisis de riesgo y el análisis de brecha, posteriormente cada área responsable de la protección de los datos personales 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 un área del IDPES.

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.

1. Medidas de Seguridad actuales:

Tipo	Mecanismo/Control	ID	Medidas actuales
Administrativas	Implementación de Políticas interna de protección de datos personales.	D1.1.1	
	Control de servidores públicos que recaban los datos personales.	D1.1.2	
	Aviso de Privacidad.	D1.1.3	
Físicas	Acceso restringido al archivo.	D2.1.1	
	Resguardar los expedientes en archiveros con llave.	D2.1.2	
	Recabar datos personales únicamente dentro de las instalaciones de cada área.	D2.1.3	
	Al concluir la jornada laboral, se deberá guardar los expedientes, para no dejarlos al alcance de ciudadanos o personal no autorizado.	D2.1.4	
Tecnológicas	Control de acceso a base de datos mediante usuario y contraseña.	D3.1.1	
	Equipo de cómputo con acceso restringido a la red de gobierno.	D3.1.2	
	Prevenir el acceso a usuarios no autorizados e identificados.	D3.1.3	
	Contar con respaldo de base de datos.	D3.1.4	

2. Análisis de Riesgos:

Medidas de seguridad actuales	ID	Riesgo/ amenaza	Factor de riesgo	Clasificación del riesgo	Control del factor	Valoración del riesgo	
						Impacto/pro babilidades Que ocurra	Valor
D1.1.1	D1.2.1						
D1.1.2	D1.2.1						
D1.1.3	D1.2.3						
D2.1.1	D2.2.1						
D2.1.2	D2.2.2						
D2.1.3	D2.2.3						
D2.1.4	D2.2.4						
D3.1.1	D3.2.1						
D3.1.2	D3.2.2						
D3.1.3	D3.2.3						
D3.1.4	D3.2.4						

3. Análisis de Brecha:

Medidas de seguridad actuales	Riesgos	ID	Identificación de la brecha
D1.1.1	D1.2.1	D1.3.1	
D1.1.2	D1.2.1	D1.3.2	
D1.1.3	D1.2.3	D1.3.3	
D2.1.1	D2.2.1	D2.3.1	
D2.1.2	D2.2.2	D2.3.2	
D2.1.3	D2.2.3	D2.3.3	
D2.1.4	D2.2.4	D2.3.4	
D3.1.1	D3.2.1	D3.3.1	
D3.1.2	D3.2.2	D3.3.2	
D3.1.3	D3.2.3	D3.3.3	
D3.1.4	D3.2.4	D3.3.4	

4. Plan de Trabajo:

Brecha que se atiende	Planificación				
	ID	Actividad	Responsable	Fecha tentativa	Evidencia entregable
D1.3.1	D1.4.1				
D1.3.2	D1.4.2				
D1.3.3	D1.4.3				
D2.3.1	D2.4.1				
D2.3.2	D2.4.2				
D2.3.3	D2.4.3				
D2.3.4	D2.4.4				
D3.3.1	D3.4.1				

D3.3.2	D3.4.2				
D3.3.3	D3.4.3				
D3.3.4	D3.4.4				

Departamento del área penal

1. Medidas de Seguridad actuales:

Tipo	Mecanismo/Control	ID	Medidas actuales
Administrativas	Implementación de Políticas interna de protección de datos personales.	P1.1.1	
	Control de servidores públicos que recaban los datos personales.	P1.1.2	
	Aviso de Privacidad.	P1.1.3	
Físicas	Acceso restringido al archivo.	P2.1.1	
	Resguardar los expedientes en archiveros con llave.	P2.1.2	
	Recabar datos personales únicamente dentro de las instalaciones de cada área.	P2.1.3	
	Al concluir la jornada laboral, se deberá guardar los expedientes, para no dejarlos al alcance de ciudadanos o personal no autorizado.	P2.1.4	
Tecnológicas	Control de acceso a base de datos mediante usuario y contraseña.	P3.1.1	
	Equipo de cómputo con acceso restringido a la red de gobierno.	P3.1.2	
	Prevenir el acceso a usuarios no autorizados e identificados.	P3.1.3	
	Contar con respaldo de base de datos.	P3.1.4	

2. Análisis de Riesgos:

Medidas de seguridad actuales	ID	Riesgo/ amenaza	Factor de riesgo	Clasificación del riesgo	Control del factor	Valoración del riesgo	
						Impacto/pro babilidades Que ocurra	Valor
P1.1.1	P1.2.1						
P1.1.2	P1.2.1						
P1.1.3	P1.2.3						
P2.1.1	P2.2.1						
P2.1.2	P2.2.2						
P2.1.3	P2.2.3						
P2.1.4	P2.2.4						
P3.1.1	P3.2.1						
P3.1.2	P3.2.2						
P3.1.3	P3.2.3						
P3.1.4	P3.2.4						

3. Análisis de Brecha:

Medidas de seguridad actuales	Riesgos	ID	Identificación de la brecha
P1.1.1	P1.2.1	P1.3.1	
P1.1.2	P1.2.1	P1.3.2	
P1.1.3	P1.2.3	P1.3.3	
P2.1.1	P2.2.1	P2.3.1	
P2.1.2	P2.2.2	P2.3.2	
P2.1.3	P2.2.3	P2.3.3	
P2.1.4	P2.2.4	P2.3.4	
P3.1.1	P3.2.1	P3.3.1	
P3.1.2	P3.2.2	P3.3.2	
P3.1.3	P3.2.3	P3.3.3	
P3.1.4	P3.2.4	P3.3.4	

4. Plan de Trabajo:

Brecha que se atiende	Planificación				
	ID	Actividad	Responsable	Fecha tentativa	Evidencia entregable
P1.3.1	P1.4.1				
P1.3.2	P1.4.2				
P1.3.3	P1.4.3				
P2.3.1	P2.4.1				
P2.3.2	P2.4.2				
P2.3.3	P2.4.3				
P2.3.4	P2.4.4				
P3.3.1	P3.4.1				
P3.3.2	P3.4.2				

P3.3.3	P3.4.3				
P3.3.4	P3.4.4				

Departamento del área civil y familiar

1. Medidas de Seguridad actuales:

Tipo	Mecanismo/Control	ID	Medidas actuales
Administrativas	Implementación de Políticas interna de protección de datos personales.	C1.1.1	
	Control de servidores públicos que recaban los datos personales.	C1.1.2	
	Aviso de Privacidad.	C1.1.3	
Físicas	Acceso restringido al archivo.	C2.1.1	
	Resguardar los expedientes en archiveros con llave.	C2.1.2	
	Recabar datos personales únicamente dentro de las instalaciones de cada área.	C2.1.3	
	Al concluir la jornada laboral, se deberá guardar los expedientes, para no dejarlos al alcance de ciudadanos o personal no autorizado.	C2.1.4	
Tecnológicas	Control de acceso a base de datos mediante usuario y contraseña.	C3.1.1	
	Equipo de cómputo con acceso restringido a la red de gobierno.	C3.1.2	
	Prevenir el acceso a usuarios no autorizados e identificados.	C3.1.3	
	Contar con respaldo de base de datos.	C3.1.4	

2. Análisis de Riesgos:

Medidas de seguridad actuales	ID	Riesgo/ amenaza	Factor de riesgo	Clasificación del riesgo	Control del factor	Valoración del riesgo	
						Impacto/probabilidades Que ocurra	Valor
C1.1.1	C1.2.1						
C1.1.2	C1.2.1						
C1.1.3	C1.2.3						
C2.1.1	C2.2.1						
C2.1.2	C2.2.2						
C2.1.3	C2.2.3						
C2.1.4	C2.2.4						
C3.1.1	C3.2.1						
C3.1.2	C3.2.2						
C3.1.3	C3.2.3						
C3.1.4	C3.2.4						

3. Análisis de Brecha:

Medidas de seguridad actuales	Riesgos	ID	Identificación de la brecha
C1.1.1	C1.2.1	C1.3.1	
C1.1.2	C1.2.1	C1.3.2	
C1.1.3	C1.2.3	C1.3.3	
C2.1.1	C2.2.1	C2.3.1	
C2.1.2	C2.2.2	C2.3.2	
C2.1.3	C2.2.3	C2.3.3	
C2.1.4	C2.2.4	C2.3.4	
C3.1.1	C3.2.1	C3.3.1	
C3.1.2	C3.2.2	C3.3.2	
C3.1.3	C3.2.3	C3.3.3	
C3.1.4	C3.2.4	C3.3.4	

4. Plan de Trabajo:

Brecha que se atiende	Planificación				
	ID	Actividad	Responsable	Fecha tentativa	Evidencia entregable
C1.3.1	C1.4.1				
C1.3.2	C1.4.2				
C1.3.3	C1.4.3				
C2.3.1	C2.4.1				
C2.3.2	C2.4.2				
C2.3.3	C2.4.3				

C2.3.4	C2.4.4				
C3.3.1	C3.4.1				
C3.3.2	C3.4.2				
C3.3.3	C3.4.3				
C3.3.4	C3.4.4				

Departamento especializado en justicia para adolescentes

1. Medidas de Seguridad actuales:

Tipo	Mecanismo/Control	ID	Medidas actuales
Administrativas	Implementación de Políticas interna de protección de datos personales.	A1.1.1	
	Control de servidores públicos que recaban los datos personales.	A1.1.2	
	Aviso de Privacidad.	A1.1.3	
Físicas	Acceso restringido al archivo.	A2.1.1	
	Resguardar los expedientes en archiveros con llave.	A2.1.2	
	Recabar datos personales únicamente dentro de las instalaciones de cada área.	A2.1.3	
	Al concluir la jornada laboral, se deberá guardar los expedientes, para no dejarlos al alcance de ciudadanos o personal no autorizado.	A2.1.4	
Tecnológicas	Control de acceso a base de datos mediante usuario y contraseña.	A3.1.1	
	Equipo de cómputo con acceso restringido a la red de gobierno.	A3.1.2	
	Prevenir el acceso a usuarios no autorizados e identificados.	A3.1.3	
	Contar con respaldo de base de datos.	A3.1.4	

2. Análisis de Riesgos:

Medidas de seguridad actuales	ID	Riesgo/ amenaza	Factor de riesgo	Clasificación del riesgo	Control del factor	Valoración del riesgo	
						Impacto/pro babilidades Que ocurra	Valor
A1.1.1	A1.2.1						
A1.1.2	A1.2.1						
A1.1.3	A1.2.3						
A2.1.1	A2.2.1						
A2.1.2	A2.2.2						
A2.1.3	A2.2.3						
A2.1.4	A2.2.4						
A3.1.1	A3.2.1						
A3.1.2	A3.2.2						
A3.1.3	A3.2.3						
A3.1.4	A3.2.4						

3. Análisis de Brecha:

Medidas de seguridad actuales	Riesgos	ID	Identificación de la brecha
A1.1.1	A1.2.1	A1.3.1	
A1.1.2	A1.2.1	A1.3.2	
A1.1.3	A1.2.3	A1.3.3	
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	
A2.1.4	A2.2.4	A2.3.4	
A3.1.1	A3.2.1	A3.3.1	
A3.1.2	A3.2.2	A3.3.2	
A3.1.3	A3.2.3	A3.3.3	
A3.1.4	A3.2.4	A3.3.4	

4. Plan de Trabajo:

Brecha que se atiende	Planificación				
	ID	Actividad	Responsable	Fecha tentativa	Evidencia entregable
A1.3.1	A1.4.1				
A1.3.2	A1.4.2				
A1.3.3	A1.4.3				
A2.3.1	A2.4.1				
A2.3.2	A2.4.2				

A2.3.3	A2.4.3				
A2.3.4	A2.4.4				
A3.3.1	A3.4.1				
A3.3.2	A3.4.2				
A3.3.3	A3.4.3				
A3.3.4	A3.4.4				

Departamento de formulación de agravios y amparo

1. Medidas de Seguridad actuales:

Tipo	Mecanismo/Control	ID	Medidas actuales
Administrativas	Implementación de Políticas interna de protección de datos personales.	F1.1.1	
	Control de servidores públicos que recaban los datos personales.	F1.1.2	
	Aviso de Privacidad.	F1.1.3	
Físicas	Acceso restringido al archivo.	F2.1.1	
	Resguardar los expedientes en archiveros con llave.	F2.1.2	
	Recabar datos personales únicamente dentro de las instalaciones de cada área.	F2.1.3	
	Al concluir la jornada laboral, se deberá guardar los expedientes, para no dejarlos al alcance de ciudadanos o personal no autorizado.	F2.1.4	
Tecnológicas	Control de acceso a base de datos mediante usuario y contraseña.	F3.1.1	
	Equipo de cómputo con acceso restringido a la red de gobierno.	F3.1.2	
	Prevenir el acceso a usuarios no autorizados e identificados.	F3.1.3	
	Contar con respaldo de base de datos.	F3.1.4	

2. Análisis de Riesgos:

Medidas de seguridad actuales	ID	Riesgo/ amenaza	Factor de riesgo	Clasificación del riesgo	Control del factor	Valoración del riesgo	
						Impacto/pro babilidades Que ocurra	Valor
F1.1.1	F1.2.1						
F1.1.2	F1.2.1						
F1.1.3	F1.2.3						
F2.1.1	F2.2.1						
F2.1.2	F2.2.2						
F2.1.3	F2.2.3						
F2.1.4	F2.2.4						
F3.1.1	F3.2.1						
F3.1.2	F3.2.2						
F3.1.3	F3.2.3						
F3.1.4	F3.2.4						

3. Análisis de Brecha:

Medidas de seguridad actuales	Riesgos	ID	Identificación de la brecha
F1.1.1	F1.2.1	F1.3.1	
F1.1.2	F1.2.1	F1.3.2	
F1.1.3	F1.2.3	F1.3.3	
F2.1.1	F2.2.1	F2.3.1	
F2.1.2	F2.2.2	F2.3.2	
F2.1.3	F2.2.3	F2.3.3	
F2.1.4	F2.2.4	F2.3.4	
F3.1.1	F3.2.1	F3.3.1	
F3.1.2	F3.2.2	F3.3.2	
F3.1.3	F3.2.3	F3.3.3	
F3.1.4	F3.2.4	F3.3.4	

4. Plan de Trabajo:

Brecha que se atiende	Planificación				
	ID	Actividad	Responsable	Fecha tentativa	Evidencia entregable
F1.3.1	F1.4.1				
F1.3.2	F1.4.2				
F1.3.3	F1.4.3				
F2.3.1	F2.4.1				
F2.3.2	F2.4.2				

F2.3.3	F2.4.3				
F2.3.4	F2.4.4				
F3.3.1	F3.4.1				
F3.3.2	F3.4.2				
F3.3.3	F3.4.3				
F3.3.4	F3.4.4				

Unidad de Transparencia

1. Medidas de Seguridad actuales:

Tipo	Mecanismo/Control	ID	Medidas actuales
Administrativas	Implementación de Políticas interna de protección de datos personales.	T1.1.1	
	Control de servidores públicos que recaban los datos personales.	T1.1.2	
	Aviso de Privacidad.	T1.1.3	
Físicas	Acceso restringido al archivo.	T2.1.1	
	Resguardar los expedientes en archiveros con llave.	T2.1.2	
	Recabar datos personales únicamente dentro de las instalaciones de cada área.	T2.1.3	
	Al concluir la jornada laboral, se deberá guardar los expedientes, para no dejarlos al alcance de ciudadanos o personal no autorizado.	T2.1.4	
Tecnológicas	Control de acceso a base de datos mediante usuario y contraseña.	T3.1.1	
	Equipo de cómputo con acceso restringido a la red de gobierno.	T3.1.2	
	Prevenir el acceso a usuarios no autorizados e identificados.	T3.1.3	
	Contar con respaldo de	T3.1.4	

	base de datos		
--	---------------	--	--

2. Análisis de Riesgos:

Medidas de seguridad actuales	ID	Riesgo/ amenaza	Factor de riesgo	Clasificación del riesgo	Control del factor	Valoración del riesgo	
						Impacto/probabilidades Que ocurra	Valor
T1.1.1	T1.2.1						
T1.1.2	T1.2.1						
T1.1.3	T1.2.3						
T2.1.1	T2.2.1						
T2.1.2	T2.2.2						
T2.1.3	T2.2.3						
T2.1.4	T2.2.4						
T3.1.1	T3.2.1						
T3.1.2	T3.2.2						
T3.1.3	T3.2.3						
T3.1.4	T3.2.4						

3. Análisis de Brecha:

Medidas de seguridad actuales	Riesgos	ID	Identificación de la brecha
T1.1.1	T1.2.1	T1.3.1	
T1.1.2	T1.2.1	T1.3.2	
T1.1.3	T1.2.3	T1.3.3	
T2.1.1	T2.2.1	T2.3.1	
T2.1.2	T2.2.2	T2.3.2	
T2.1.3	T2.2.3	T2.3.3	
T2.1.4	T2.2.4	T2.3.4	
T3.1.1	T3.2.1	T3.3.1	
T3.1.2	T3.2.2	T3.3.2	
T3.1.3	T3.2.3	T3.3.3	
T3.1.4	T3.2.4	T3.3.4	

4. Plan de Trabajo:

Brecha que se atiende	Planificación				
	ID	Actividad	Responsable	Fecha tentativa	Evidencia entregable
T1.3.1	T1.4.1				
T1.3.2	T1.4.2				
T1.3.3	T1.4.3				

T2.3.1	T2.4.1				
T2.3.2	T2.4.2				
T2.3.3	T2.4.3				
T2.3.4	T2.4.4				
T3.3.1	T3.4.1				
T3.3.2	T3.4.2				
T3.3.3	T3.4.3				
T3.3.4	T3.4.4				

XII. Mecanismos de Monitoreo.

De conformidad a lo dispuesto por la LPDPPSOES, para la protección de datos personales, el IDPES 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 área, se estará solicitando copia de la evidencia que sustente las actividades realizadas. Posteriormente, en la actualización anual que corresponda, se estará trabajando con las titulares de cada área, 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.

Presentar al área responsable de la capacitación en la Institución, una propuesta para que se integren al programa de capacitación institucional los cursos necesarios para difundir los conceptos e importancia de la seguridad de la información, protección de datos personales y avisos de privacidad.

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.

Estas modificaciones se realizarán y efectuarán, previa solicitud a la Dirección del IDPES por parte de las áreas 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 del área deberá dar aviso a la Dirección del IDPES 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 de la Defensoría Pública del Estado de Sinaloa, en Sesión Ordinaria realizada el día 17 de julio de 2020.

QUINTA SESIÓN ORDINARIA DEL COMITÉ DE TRANSPARENCIA DEL INSTITUTO DE LA DEFENSORÍA PÚBLICA DEL ESTADO DE SINALOA QUE APRUEBA EL DOCUMENTO DE SEGURIDAD EN MATERIA DE TRATAMIENTO DE DATOS PERSONALES EN POSESIÓN DEL INSTITUTO DE LA DEFENSORÍA PÚBLICA DEL ESTADO DE SINALOA.

--- En la Ciudad de Culiacán Rosales, Sinaloa, siendo las 10:00 a.m. (diez horas) del día viernes (diecisiete) de julio del año 2020 (dos mil veinte), constituidos en el área que ocupa la Dirección del Instituto de Defensoría Pública Sinaloa ubicadas en Boulevard Rolando Arjona s/n, Colonia Juntas del Humaya, en esta Ciudad capital; reunidos para celebrar formal sesión del Comité de Transparencia del Instituto de Defensoría Pública Sinaloa, **con el fin de aprobar el Documento de Seguridad en Materia de Tratamiento de Datos Personales en Posesión del Instituto de la Defensoría Pública del Estado de Sinaloa, así pues, con fundamento en lo dispuesto por el artículo 111, fracciones I y II de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Sinaloa; se reúnen los integrantes del Comité de Transparencia del Instituto de Defensoría Pública; encontrándose presentes la C. Yeli Karina Burgos León, Jefa del Departamento Especializado en Justicia para Adolescentes (Presidenta); C. Alejandro Acuña Montoya, Jefe del Departamento de Formulación de Agravios y Amparo, (Integrante) y C. Emma Eutimía Navarro Zazueta, Jefa del Departamento Civil y Familiar (Integrante); para analizar el planteamiento expuesto por la Responsable de la Unidad de Transparencia al caso que nos ocupa; y,**-----

CONSIDERANDO

---Que la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Sinaloa, establece que el Comité de Transparencia es aquella instancia a la que hace referencia el artículo 61 de la Ley de Transparencia y Acceso a la Información Pública y dicho artículo dice que es el órgano colegiado que se integrará en cada uno de los sujetos obligados que deberá de estar integrado por un número impar de servidores públicos y, en su caso, de personas designadas por su Titular.

--Que 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.

-Que la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Sinaloa puntualiza que el Comité de Transparencia será la autoridad máxima en materia de protección de datos personales, en la organización del responsable.

-Que una de las facultades del Comité de Transparencia es la de aprobar, supervisar y evaluar las políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la Ley de Protección de Datos Personales y demás disposiciones que resulten aplicables a la materia. Asimismo es potestad del mismo Comité el coordinar, realizar y supervisar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable.

--Que sobre las consideraciones anteriores y en observancia a lo que establecen las Leyes previamente mencionadas, la Responsable de la Unidad de Transparencia señala la importancia de la creación del "Documento de Seguridad en Materia de Tratamiento de Datos Personales en Posesión del Instituto de la Defensoría Pública del Estado de Sinaloa" y a petición expresa de las áreas responsables de la Protección de Datos Personales, lo anterior de acuerdo a las fracciones I y II del artículo 111 de la Ley de Protección de Datos Personales debe de ser aprobado por el Comité de Transparencia.

--Así pues, el documento a aprobar aduce que 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".

-Sigue manifestando que a partir de la publicación de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Sinaloa y los Lineamientos de Protección de Datos Personales para Sujetos Obligados del Estado de Sinaloa, el Instituto de la Defensoría Pública 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 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.

-Que entre los "Deberes" previstos en la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Sinaloa, el Instituto de la Defensoría Pública 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 del Instituto de la Defensoría Pública del Estado de Sinaloa coordinó la elaboración de dicho documento, para cumplir con los que se establece en los artículos 35 de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados y 42 de la Ley de Protección de Datos Personales local.

---Que tras analizar el Documento de Seguridad en Materia de Tratamiento de Datos Personales en Posesión del Instituto de la Defensoría Pública 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 los Sujetos Obligados del Estado de Sinaloa, por unanimidad resuelve emitir los siguientes:

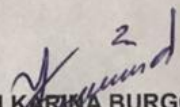
ACUERDOS

---PRIMERO.-Se aprueban el Documento de Seguridad en Materia de Tratamiento de Datos Personales en Posesión del Instituto de la Defensoría Pública del Estado de Sinaloa.

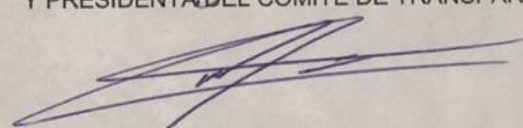
---SEGUNDO.-Se instruye a la Titular de la Unidad de Transparencia del Instituto de la Defensoría Pública del Estado de Sinaloa dar a conocer a los servidores públicos adscritos a este Instituto el documento aprobado y manifestarles la importancia de su observación y cumplimiento.

- - - Lo anterior se acordó por unanimidad del Comité de Transparencia del Instituto de la Defensoría Pública del Estado de Sinaloa.

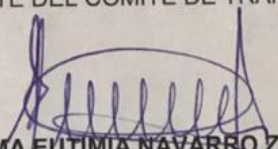
---Se da por concluida la presente acta, siendo las 10:30 a.m. (diez treinta horas) del día en que se actúa; firmando al calce y margen los intervinientes e integrantes presentes del Comité de Transparencia del Instituto de la Defensoría Pública del Estado de Sinaloa, para los efectos legales a que haya lugar.


C. YELI KARINA BURGOS LEON.

JEFA DEL DEPARTAMENTO ESPECIALIZADO EN JUSTICIA PARA ADOLESCENTES
Y PRESIDENTA DEL COMITÉ DE TRANSPARENCIA.


C. ALEJANDRO ACUÑA MONTOYA.

JEFE DE DEPARTAMENTO DE FORMULACION DE AGRAVIOS Y AMPARO E
INTEGRANTE DEL COMITÉ DE TRANSPARENCIA.


C. EMMA EUTIMIA NAVARRO ZAZUETA.

JEFA DEL DEPARTAMENTO DEL AREA CIVIL Y FAMILIAR E INTEGRANTE DEL
COMITÉ DE TRANSPARENCIA.