DOCUMENTO DE SEGURIDAD

EN MATERIA DE TRATAMIENTO DE DATOS PERSONALES
EN POSESIÓN DEL INSTITUTO SINALOENSE
PARA LA EDUCACIÓN DE LOS JÓVENES Y ADULTOS.

CONTENIDO

I. INTRODUCCIÓN. 5

II. MARCO NORMATIVO. 7

III. ÁMBITO DE APLICACIÓN. 8

IV. POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES DEL INSTITUTO SINALOENSE PARA LA EDUCACIÓN DE LOS JÓVENES Y ADULTOS. 9

Objeto. 9

A. Responsable del Tratamiento de los Datos Personales y Fundamento para ello. 9

B. Datos Sometidos a Tratamiento. 9

C. Derechos de los Titulares de los Datos Personales. 11

D. Área responsable de la implementación y observancia de esta política. 12

E. Autorización – Consentimiento. 12

F. Seguridad de los Datos Personales. 14

G. Tratamiento de Datos Personales. 14

H. Vigencia. 15

V. FUNCIONES Y OBLIGACIONES DEL PERSONAL INVOLUCRADO EN EL TRATAMIENTO DE DATOS PERSONALES. 16

VI. INVENTARIOS DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO 16

Coordinación Regional. 18

Departamento de Administración y Finanzas 23

Departamento de Planeación y Seguimiento Operativo 28

Departamento de Acreditación 33

Departamento de Servicios Educativos 38

Departamento de Sistemas 43

Unidad de Asuntos Jurídicos 48

Unidad de Transparencia 53

VII. MEDIDAS DE SEGURIDAD. 58

VIII. ANÁLISIS DE RIESGOS. 62

IX. ANÁLISIS DE BRECHA. 64

X. PLAN DE TRABAJO. 64

XI. METODOLOGÍA PARA LA REDACCIÓN Y VINCULACIÓN DE LA INFORMACIÓN..... 64
Coordinación Regional..... 66
1. Medidas de Seguridad actuales:..... 66
2. Análisis de Riegos: 67
3. Análisis de Brecha: 67
4.- Plan de Trabajo: 67
Departamento de Administración y Finanzas..... 68
1. Medidas de Seguridad actuales:..... 68
2. Análisis de Riegos: 69
3. Análisis de Brecha: 69
4.- Plan de Trabajo: 70
Departamento de Planeación y Seguimiento operativo 71
1. Medidas de Seguridad actuales:..... 71
2. Análisis de Riegos: 72
3. Análisis de Brecha: 72
4.- Plan de Trabajo: 72
Departamento de Acreditación..... 73
1. Medidas de Seguridad actuales:..... 73
2. Análisis de Riegos: 74
3. Análisis de Brecha: 74
4.- Plan de Trabajo: ..... **¡Error! Marcador no definido.**
Departamento de Servicios Educativos 75
1. Medidas de Seguridad actuales:..... 76
2. Análisis de Riegos: 77
3. Análisis de Brecha: 77
4.- Plan de Trabajo: 78
Departamento de Sistemas..... 79
1. Medidas de Seguridad actuales:..... 79
2. Análisis de Riegos: 80
3. Análisis de Brecha: 80

4.- Plan de Trabajo: 81
Unidad de Asuntos Jurídicos 82
1. Medidas de Seguridad actuales: 82
2. Análisis de Riegos: 83
3. Análisis de Brecha: 83
4.- Plan de Trabajo: 83
Unidad de Transparencia 84
1. Medidas de Seguridad actuales: 84
2. Análisis de Riegos: 85
3. Análisis de Brecha: 85
4.- Plan de Trabajo: 85
XII. MECANISMOS DE MONITOREO. 86
XIII. PROGRAMA GENERAL DE CAPACITACIÓN. 86
XIV. ACTUALIZACIONES 86
Aprobación 87

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 Sinaloense para la Educación de los Jóvenes y Adultos en el Estado de Sinaloa (ISEJA) 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 ISEJA, 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 Unidad de Transparencia coordinó la elaboración de este documento.

II. Marco Normativo.

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

- Artículos 6 y 16 de la Constitución Política de los Estados Unidos Mexicanos.
- Ley General de Transparencia y Acceso a la Información Pública (LGTAIP).
- Ley General de Protección de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO).
- Ley de Transparencia y Acceso a la Información Pública del Estado de Sinaloa (LTAIPES).
- Ley Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Sinaloa (LPDPPSOES).
- Lineamientos de Protección de Datos Personales para Sujetos Obligados del Estado de Sinaloa.
- Decreto de Creación del Instituto Sinaloense Para la Educación de los Adultos.
- Decreto por el que se Reforman, Adicionan y Deroga diversas disposiciones al Decreto que Crea al Instituto Sinaloense para la Educación de los Adultos. (Cambio de nombre a ISEJA), entre otras.

III. Ámbito de aplicación.

En atención a los “Deberes” que refiere la LPDPSOES, el presente documento es aplicable para todas las áreas del ISEJA, 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 Sinaloense para la Educación de los Jóvenes y Adultos.

El ISEJA, 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 ISEJA 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 y 196 fracción VIII de la LPDPPSOES.

B. Datos Sometidos a Tratamiento.

Los datos personales serán utilizados con la finalidad de:

a) La vinculación y la gestión del Instituto con el sector público, privado y social.
b) El registro, contratación y gestión de personal que labora en el Instituto, particularmente expedientes laborales.
c) La celebración de contratos, convenios y adjudicaciones.
d) El registro de proveedores dentro de un catálogo.

e) Llevar a cabo un seguimiento operativo y estadístico del Instituto y todas las figuras operativas que participan en el proceso educativo.
f) La elaboración de planes y programas estadísticos, proyecciones financieras, entre otras.
g) La inscripción, acreditación y certificación, diagnósticos y avances académicos, así como para la emisión de reportes estadísticos.
h) Transferir datos personales a las autoridades, poderes, entidades, órganos y organismos gubernamentales de los tres órdenes de gobierno, así como instituciones internacionales dedicadas al ámbito de la educación y la cultura para las siguientes finalidades: • Para estudios de investigación educativa nacional, regional o local, que realicen la Secretaría de Educación Pública, Instituciones Públicas Educativas Nacionales y Estatales, así como Organismos Internacionales en el ámbito de la educación y la cultura. • Para atender requerimientos de información de una autoridad competente, que estén debidamente fundados y motivados.
i) Para contactos posteriores de acciones relacionadas con su aprovechamiento académico.
j) El seguimiento educativo, avances académicos y asesorías en cuanto a los usuarios del Servicio de Educación para Adultos, así como también para la implementación y desarrollo de programas de capacitación para el personal del Instituto y figuras académicas que requieran de la formación en sus diferentes niveles.
k) Para el seguimiento educativo, avances académicos y estadísticas educativas; todo ello en virtud de una base de datos.
l) La elaboración de documentación jurídica ya conocida por las personas otorgantes, así como asesorías y trámites internos de las diferentes áreas que conforman el Instituto.
m) Comunicarnos con la persona/usuario, en caso de que sea necesario en razón de alguna solicitud de acceso a la información pública y/o de datos personales.

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

1) Nombre completo.
2) Datos Laborales (currículo, referencias laborales y personales, correo electrónico, CURP, RFC, comprobante de domicilio y teléfono particular).
3) Al usuario: adicionalmente documentación escolar, acta de nacimiento, fotografías, comprobante de domicilio)
4) Edad.
5) Domicilio.
6) Nivel de escolaridad.
7) Referencias Personales, así como nombre de cónyuge, nombre del padre, nombre de la madre y datos personales de sus dependientes económicos.
8) Institución bancaria, número de cuenta y clabe interbancaria.

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

C. Derechos de los Titulares de los Datos Personales.

Para el ejercicio de cualquiera de los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO), se deberá presentar la solicitud respectiva en el Instituto Sinaloense para la Educación de los Jóvenes y Adultos, con domicilio en Boulevard Ciudades Hermanas #665 oriente, colonia Antonio Rosales, Culiacán, Sinaloa, C.P.80200.

Para conocer el procedimiento y requisitos para el ejercicio de los derechos ARCO, se podrá llamar al siguiente número telefónico (667)715-03-32 Extensión 525; 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: domicilio en Boulevard Ciudades Hermanas #665 oriente, colonia Antonio Rosales, Culiacán, Sinaloa, C.P.80200. Teléfono: (667)715-03-32 ext. 525.

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

El Instituto Sinaloense para la Educación de los Jóvenes y Adultos, a través del responsable de la Unidad de Transparencia, 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 ISEJA, 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 ISEJA, se limita a disponer de los medios adecuados para este fin.

El ISEJA, 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 ISEJA.

G. Tratamiento de Datos Personales.

El ISEJA, deberá darles 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 ISEJA.

IV. 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.

V. 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 Departamento y en orden con base a la Estructura Orgánica del ISEJA.

A. Coordinación Regional.

B. Departamento de Administración y Finanzas.
C. Departamento de Planeación y Seguimiento Operativo.
D. Departamento de Acreditación.
E. Departamento de Servicios Educativos.
F. Departamento de Sistemas
G. Unidad de Asuntos Jurídicos.
H. Unidad de Transparencia.

En los siguientes apartados, se estará abordando cada uno de los sistemas señalando su descripción, estructura y medidas se 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 el Departamento, 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.

Coordinación Regional.

1.- Fundamento Legal. – Capítulo cuarto, Artículo 12 del Decreto de Creación del Instituto Sinaloense Para la Educación de los Jóvenes y Adultos.

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

SINALOA
GOBIERNO DEL ESTADO

ISEJA
INSTITUTO SINALOENSE PARA LA EDUCACIÓN DE LOS JÓVENES Y ADULTOS

INVENTARIO DE DATOS PERSONALES GENERALES

DEPARTAMENTO DE COORDINACION REGIONAL

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 Área.

Datos Personales Recabados	Existente	Necesario	No necesario
Datos de identificación y contacto			
Nombre	x	x	
Alias	x		x
Seudónimo	x		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	x	
Firma autógrafa	x	x	
Firma electrónica	x	x	
Edad	x	x	
Fotografía	x	x	
Referencias personales	x		x
Escolaridad	x	x	
Número de seguridad social o análogo	x		x

Datos sobre características físicas			
Color de piel			
Color de cabello			
Señas particulares			
Estatura			
Peso			
Cicatrices			
Tipo de sangre			
Datos Personales Recabados	**Existente**	**Necesario**	**No necesario**
Imagen de iris			
Huella dactilar			
Palma de la mano			
ADN (Código genético)			
Datos laborales			
Puesto o cargo que desempeña	x	x	
Domicilio del trabajo	x	x	
Correo electrónico institucional	x	x	
Teléfono institucional	x	x	
Referencia laborales	x	x	
Información generada durante los procedimientos de reclutamiento; selección y contratación	x		x
Experiencia/Capacitación laboral	x		x
Datos académicos			
Trayectoria educativa	x	x	
Títulos	x	x	
Cedula profesional	x	x	
Certificados	x	x	
Reconocimientos	x	x	
Datos migratorios			
Entrada al país			
Salida de país			
Tiempo de permanencia en el país			
Calidad migratoria			
Derechos de residencia			
Aseguramiento			
Repatriación			

Datos patrimoniales y/o financieros			
Bienes muebles	x	x	
Bienes inmuebles	x	x	
Información fiscal			
Historial crediticio/Buró de crédito			
Ingresos			
Egresos			
Cuentas bancarias			
Números de tarjetas de crédito			
Información adicional de tarjeta (fechas de vencimiento, códigos de seguridad, datos de banda magnética, pin)			
Seguros			
Afores			
Datos sobre pasatiempos, entretenimientos y diversión			
Datos Personales Recabados	**Existente**	**Necesario**	**No necesario**
Pasatiempos			
Aficiones			
Deportes de practica			
Juegos de su interés			
Datos legales			
Situación jurídica de la persona (juicios, amparos, procesos administrativos, entre otros)			
Otros datos personales (mencionar)			

Área: COORDINACION REGIONAL

Nombre: ING. L. BLADIMIR MARTINEZ ESPINOZA

Firma: _____

"Este programa es público ajeno a cualquier partido político, queda prohibido el uso para fines distintos a los establecidos en el programa". Quién haga uso indebido de los recursos de este programa deberá ser denunciado/a y sancionado/a de acuerdo con la ley aplicable y ante la autoridad competente".

INVENTARIO DE DATOS PERSONALES SENSIBLES

DEPARTAMENTO DE: COORDINACION REGIONAL

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 Área.

Datos personales recabados	Existente	Necesario	No necesario
Datos de identificación y contacto			
Posturas religiosas/ ideológicas/morales/filosóficas			
Pertenencia a un partido/Posturas políticas			
Pertenencia a un sindicato	x		x
Datos de Salud			
Estado de salud físico presente, pasado o futuro			
Estado de salud mental presente, pasado o 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			
Otros datos personales (mencionar)			

Área: COORDINACION REGIONAL

Nombre: ING. L. BLADIMIR MARTINEZ ESPINOZA

Firma: _____

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

4.- Servidor Público Administrador de la Coordinación:

Cargo: Coordinador Regional

Teléfono y Extensión: 667 715-0332 Ext 508.

Funciones/Perfil: Cumplir con las funciones que correspondan al puesto de conformidad con el Decreto de Creación del ISEJA y realizar aquellas que le encomienden sus superiores jerárquicos.

Obligaciones: Entre otras, gestión y vinculación con el sector público, privado y social; así como coordinar administrativamente a las coordinaciones de zona.

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

6.- Características del lugar donde se resguardan los sistemas de tratamiento de datos personales. – La Coordinación Regional del ISEJA, se encuentra en: Boulevard Ciudades Hermanas #665 oriente, colonia Antonio Rosales, C.P.80200, en Culiacán, Sinaloa.
Los archivos físicos se encuentran en una oficina con acceso restringido, solo se autoriza personal de la coordinación y están depositados en archiveros con llave.

7.- Portabilidad de datos. - La Coordinación Regional, no cuenta con ningún formato estructurado para la portabilidad de datos.

8.- Transferencia de datos. - La Coordinación Regional, no transfiere los datos personales.

9.- Encargado de datos. - Coordinación Regional.

Departamento de Administración y Finanzas

1.- Fundamento Legal. – Capítulo cuarto, Artículo 12 del Decreto de Creación del Instituto Sinaloense Para la Educación de los Jóvenes y Adultos.

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

SINALOA
GOBIERNO DEL ESTADO

ISEJA
INSTITUTO SINALOENSE PARA LA EDUCACIÓN DE LOS JÓVENES Y ADULTOS

INVENTARIO DE DATOS PERSONALES GENERALES

DEPARTAMENTO DE ADMINISTRACIÓN Y FINANZAS

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 Área.

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
Teléfono celular personal	X	X	
Correo electrónico personal	X	X	
Firma autógrafa	X	X	
Firma electrónica			X
Edad	X	X	
Fotografía	X	X	
Referencias personales	X		X
Escolaridad	X	X	
Número de seguridad social o análogo	X	X	

Datos sobre características físicas			
Color de piel			X
Color de cabello			X
Señas particulares			X
Estatura			X
Peso			X
Cicatrices			X
Tipo de sangre			X
Datos biomédicos			
Datos Personales Recabados	**Existente**	**Necesario**	**No necesario**
Imagen de iris			**X**
Huella dactilar	X		X
Palma de la mano			X
ADN (Código genético)			X
Datos laborales			
Puesto o cargo que desempeña	X	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	X	
Experiencia/Capacitación laboral	X	X	
Datos académicos			
Trayectoria educativa	X	X	
Títulos	X	X	
Cedula profesional	X	X	
Certificados	X	X	
Reconocimientos			X
Datos migratorios			
Entrada al país			X
Salida de país			X
Tiempo de permanencia en el país			X
Calidad migratoria			X
Derechos de residencia			X
Aseguramiento			X
Repatriación			X

Datos patrimoniales y/o financieros			
Bienes muebles	X	X	
Bienes inmuebles	X	X	
Información fiscal	X	X	
Historial crediticio/Buró de crédito		X	
Ingresos	X	X	
Egresos	X	X	
Cuentas bancarias	X	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		X
Afores	X		X
Datos sobre pasatiempos, entretenimientos y diversión			
Datos Personales Recabados	**Existente**	**Necesario**	**No necesario**
Pasatiempos			X
Aficiones			X
Deportes de practica			X
Juegos de su interés			X
Datos legales			
Situación jurídica de la persona (juicios, amparos, procesos administrativos, entre otros)			X
Otros datos personales (mencionar)			

Área: Departamento de Administración y Finanzas

Nombre: Dr. Oracio Valenzuela Valenzuela

Firma: _____

INVENTARIO DE DATOS PERSONALES SENSIBLES

DEPARTAMENTO DE ADMINISTRACIÓN Y FINANZAS

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 Área.

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	X	
Estado de salud mental presente, pasado o futuro			X
Información genética			X
Datos sobre vida sexual			
Preferencias sexuales			X
Practicas 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)			

Área: Departamento de Administración y Finanzas

Nombre: Dr. Oracio Valenzuela Valenzuela

Firma: _____

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

4.- Servidor Público Administrador del Departamento:

Cargo: Jefe del Departamento

Teléfono y Extensión: 667 715-0332 Ext 505

Funciones/Perfil: Cumplir con las funciones que correspondan al puesto de conformidad con el Decreto de Creación del ISEJA y realizar aquellas que le encomienden sus superiores jerárquicos.

Obligaciones: Entre otras, La contratación del personal, así como celebración de contratos de prestación de servicios, adjudicaciones; administración de bienes y servicios, control patrimonial bienes muebles, etc.

5.- Tipo de Soporte. - El soporte de los datos personales se encuentran en físico y de manera electrónica.

6.- Características del lugar donde se resguardan los sistemas de tratamiento de datos personales. – El Departamento de Administración y Finanzas del ISEJA, se encuentra en: Boulevard Ciudades Hermanas #665 oriente, colonia Antonio Rosales, C.P.80200, en Culiacán, Sinaloa.

Los archivos físicos se encuentran en una oficina con acceso restringido, solo se autoriza personal de la coordinación y están depositados en archiveros con llave.

7.- Portabilidad de datos. – El Departamento de Administración y Finanzas, no cuenta con ningún formato estructurado para la portabilidad de datos.

8.- Transferencia de datos. - El Departamento de Administración y Finanzas, no transfiere los datos personales.

9.- Encargado de datos. - . El Departamento de Administración y Finanzas.

Departamento de Planeación y Seguimiento Operativo

1.- Fundamento Legal. – Capítulo cuarto, Artículo 12 del Decreto de Creación del Instituto Sinaloense Para la Educación de los Jóvenes y Adultos.

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

SINALOA
GOBIERNO DEL ESTADO

ISEJA
INSTITUTO SINALOENSE PARA LA EDUCACIÓN DE LOS JÓVENES Y ADULTOS

INVENTARIO DE DATOS PERSONALES GENERALES

DEPARTAMENTO DE PLANEACIÓN Y SEGUIMIENTO OPERATIVO

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 Área.

Datos Personales Recabados	Existente	Necesario	No necesario
Datos de identificación y contacto			
Nombre	X	X	
Alias			
Seudónimo			
Sexo			
Estado Civil			
Registro Federal de Contribuyentes (RFC)	X	X	
Registro Federal del instituto Nacional (INE)			
Clave Única de Registro de Población (CURP)	X	X	
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 biomédicos			
Datos Personales Recabados	**Existente**	**Necesario**	**No necesario**
Imagen de iris			
Huella dactilar			
Palma de la mano			
ADN (Código genético)			
Datos laborales			
Puesto o cargo que desempeña	X	X	
Domicilio del trabajo	X	X	
Correo electrónico institucional	X	X	
Teléfono institucional	X	X	
Referencia laborales	X	X	
Información generada durante los procedimientos de reclutamiento; selección y contratación			
Experiencia/Capacitación laboral			
Datos académicos			
Trayectoria educativa			
Títulos			
Cedula profesional			
Certificados			
Reconocimientos			
Datos migratorios			
Entrada al país			
Salida de país			
Tiempo de permanencia en el país			
Calidad migratoria			
Derechos de residencia			

"Este programa es público ajeno a cualquier partido político, queda prohibido el uso para fines distintos a los establecidos en el programa". Quién haga uso indebido de los recursos de este programa deberá ser denunciado/a y sancionado/a de acuerdo con la ley aplicable y ante la autoridad competente".

Aseguramiento			
Repatriación			
Datos patrimoniales y/o financieros			
Bienes muebles			
Bienes inmuebles			
Información fiscal			
Historial crediticio/Buró de crédito			
Ingresos			
Egresos			
Cuentas bancarias			
Números de tarjetas de crédito			
Información adicional de tarjeta (fechas de vencimiento, códigos de seguridad, datos de banda magnética, pin)			
Seguros			
Afores			
Datos sobre pasatiempos, entretenimientos y diversión			
Datos Personales Recabados	**Existente**	**Necesario**	**No necesario**
Pasatiempos			
Aficiones			
Deportes de practica			
Juegos de su interés			
Datos legales			
Situación jurídica de la persona (juicios, amparos, procesos administrativos, entre otros)			
Otros datos personales (mencionar)			

Área: DEPARTAMENTO DE PLANEACIÓN Y SEGUIMIENTO OPERATIVO

Nombre: LIC. JOSÉ LUIS AVARADO MEDRANO

Firma: _____

ISEJA
INSTITUTO SINALOENSE PARA LA EDUCACIÓN DE LOS JÓVENES Y ADULTOS

DEPARTAMENTO DE PLANEACIÓN

"Este programa es público ajeno a cualquier partido político, queda prohibido el uso para fines distintos a los establecidos en el programa". Quién haga uso indebido de los recursos de este programa deberá ser denunciado/a y sancionado/a de acuerdo con la ley aplicable y ante la autoridad competente".

INVENTARIO DE DATOS PERSONALES SENSIBLES

DEPARTAMENTO DE PLANEACIÓN Y SEGUIMIENTO OPERATIVO

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 Área.

Datos personales recabados	Existente	Necesario	No necesario
Datos de identificación y contacto			
Posturas religiosas/ ideológicas/morales/filosóficas			
Pertenencia a un partido/Posturas políticas			
Pertenencia a un sindicato	X	X	
Datos de Salud			
Estado de salud físico presente, pasado o futuro			
Estado de salud mental presente, pasado o 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			
Otros datos personales (mencionar)			

Área: DEPARTAMENTO DE PLANEACIÓNY SEGUIMIENTO OPERATIVO

Nombre: LIC. JOSÉ LUIS ALVARADO MEDRANO

Firma: _____

ISEJA
DEPARTAMENTO DE PLANEACIÓN

"Este programa es público ajeno a cualquier partido político, queda prohibido el uso para fines distintos a los establecidos en el programa". Quién haga uso indebido de los recursos de este programa deberá ser denunciado/a y sancionado/a de acuerdo con la ley aplicable y ante la autoridad competente".

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

4.- Servidor Público Administrador del Departamento:

Cargo: Jefe del Departamento

Teléfono y Extensión: 667 715-0332 Ext 509

Funciones/Perfil: Cumplir con las funciones que correspondan al puesto de conformidad con el Decreto de Creación del ISEJA y realizar aquellas que le encomienden sus superiores jerárquicos.

Obligaciones: Entre otras, el seguimiento operativo, proyectos estadísticos y la coordinación con instituciones educativas, servicio social, etc.

5.- Tipo de Soporte. - El soporte de los datos personales se encuentran en físico y de manera electrónica.

6.- Características del lugar donde se resguardan los sistemas de tratamiento de datos personales. – El Departamento de Planeación y Seguimiento Operativo del ISEJA, se encuentra en: Boulevard Ciudades Hermanas #665 oriente, colonia Antonio Rosales, C.P.80200, en Culiacán, Sinaloa.
Los archivos físicos se encuentran en una oficina con acceso restringido, solo se autoriza personal de la coordinación y están depositados en archiveros con llave.

7.- Portabilidad de datos. – El Departamento de Planeación y Seguimiento Operativo, no cuenta con ningún formato estructurado para la portabilidad de datos.

8.- Transferencia de datos. - El Departamento de Planeación y Seguimiento Operativo, no transfiere los datos personales.

9.- Encargado de datos. - . El Departamento de Planeación y Seguimiento Operativo.

Departamento de Acreditación

1.- Fundamento Legal. – Capítulo cuarto, Artículo 12 del Decreto de Creación del Instituto Sinaloense Para la Educación de los Jóvenes y Adultos.

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

SINALOA
GOBIERNO DEL ESTADO

ISEJA
INSTITUTO SINALOENSE PARA LA EDUCACIÓN DE LOS JÓVENES Y ADULTOS

INVENTARIO DE DATOS PERSONALES GENERALES

DEPARTAMENTO DE ACREDITACION

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 Área.

Datos Personales Recabados	Existente	Necesario	No necesario
Datos de identificación y contacto			
Nombre	X		
Alias			X
Seudónimo			X
Sexo	X		
Estado Civil	X		
Registro Federal de Contribuyentes (RFC)	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		
Teléfono particular	X		
Teléfono celular personal	X		
Correo electrónico personal	X		
Firma autógrafa	X		
Firma electrónica	X		
Edad	X		
Fotografía	X		
Referencias personales	X		
Escolaridad	X		
Número de seguridad social o análogo			X

Datos sobre características físicas			
Color de piel			X
Color de cabello			X
Señas particulares			X
Estatura			X
Peso			X
Cicatrices			X
Tipo de sangre			X
Datos biomédicos			
Datos Personales Recabados	**Existente**	**Necesario**	**No necesario**
Imagen de iris			**X**
Huella dactilar			X
Palma de la mano			X
ADN (Código genético)			X
Datos laborales			
Puesto o cargo que desempeña	X		
Domicilio del trabajo	X		
Correo electrónico institucional	X		
Teléfono institucional	X		
Referencia laborales	X		
Información generada durante los procedimientos de reclutamiento; selección y contratación	X		
Experiencia/Capacitación laboral	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		

"Este programa es público ajeno a cualquier partido político, queda prohibido el uso para fines distintos a los establecidos en el programa". Quién haga uso indebido de los recursos de este programa deberá ser denunciado/a y sancionado/a de acuerdo con la ley aplicable y ante la autoridad competente".

Repatriación	X		
Datos patrimoniales y/o financieros			
Bienes muebles			X
Bienes inmuebles			X
Información fiscal			X
Historial crediticio/Buró de crédito			X
Ingresos			X
Egresos			X
Cuentas bancarias			X
Números de tarjetas de crédito			X
Información adicional de tarjeta (fechas de vencimiento, códigos de seguridad, datos de banda magnética, pin)			X
Seguros			X
Afores			X
Datos sobre pasatiempos, entretenimientos y diversión			
Datos Personales Recabados	**Existente**	**Necesario**	**No necesario**
Pasatiempos			X
Aficiones			X
Deportes de practica			X
Juegos de su interés			X
Datos legales			
Situación jurídica de la persona (juicios, amparos, procesos administrativos, entre otros)		X	
Otros datos personales (mencionar)			

Área: ACREDITACION

Nombre: RUBEN ANTONIO GONZALEZ FRANCO

Firma:

INVENTARIO DE DATOS PERSONALES SENSIBLES

DEPARTAMENTO DE ACREDITACION

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 Área.

Datos personales recabados	Existente	Necesario	No necesario
Datos de identificación y contacto			
Posturas religiosas/ ideológicas/morales/filosóficas			X
Pertenencia a un partido/Posturas políticas			X
Pertenencia a un sindicato			X
Datos de Salud			
Estado de salud físico presente, pasado o futuro			X
Estado de salud mental presente, pasado o futuro			X
Información genética			X
Datos sobre vida sexual			
Preferencias sexuales			X
Practicas 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)			
			X

Área: ACREDITACION

Nombre: RUBEN ANTONIO GONZALEZ FRANCO

Firma:

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

4.- Servidor Público Administrador del Departamento:

Cargo: Jefe del Departamento

Teléfono y Extensión: 667 715-0332 Ext 521

Funciones/Perfil: Cumplir con las funciones que correspondan al puesto de conformidad con el Decreto de Creación del ISEJA y realizar aquellas que le encomienden sus superiores jerárquicos.

Obligaciones: Entre otras, la inscripción, acreditación y certificación de los servicios de Educación para Adultos. etc.

5.- Tipo de Soporte. - El soporte de los datos personales se encuentran en físico y de manera electrónica.

6.- Características del lugar donde se resguardan los sistemas de tratamiento de datos personales. – El Departamento de Acreditación del ISEJA, se encuentra en: Boulevard Ciudades Hermanas #665 oriente, colonia Antonio Rosales, C.P.80200, en Culiacán, Sinaloa.

Los archivos físicos se encuentran en una oficina con acceso restringido, solo se autoriza personal del Departamento y están depositados en archiveros con llave.

7.- Portabilidad de datos. – El Departamento de Acreditación, no cuenta con ningún formato estructurado para la portabilidad de datos.

8.- Transferencia de datos. - El Departamento de Acreditación, no transfiere los datos personales.

9.- Encargado de datos. - . El Departamento de Acreditación.

Departamento de Servicios Educativos

1.- Fundamento Legal. – Capítulo cuarto, Artículo 12 del Decreto de Creación del Instituto Sinaloense Para la Educación de los Jóvenes y Adultos.

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

SINALOA
GOBIERNO DEL ESTADO

ISEJA
INSTITUTO SINALOENSE PARA LA EDUCACIÓN DE LOS JÓVENES Y ADULTOS

INVENTARIO DE DATOS PERSONALES GENERALES

DEPARTAMENTO DE SERVICIOS EDUCATIVOS

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 Área.

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
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	X	
Firma autógrafa	X	X	
Firma electrónica			X
Edad	X	X	
Fotografía			X
Referencias personales			X
Escolaridad	X	X	
Número de seguridad social o análogo	X	X	

Datos sobre características físicas			
Color de piel			X
Color de cabello			X
Señas particulares			X
Estatura			X
Peso			X
Cicatrices			X
Tipo de sangre			X
Datos biomédicos			
Datos Personales Recabados	**Existente**	**Necesario**	**No necesario**
Imagen de iris			X
Huella dactilar			X
Palma de la mano			X
ADN (Código genético)			X
Datos laborales			
Puesto o cargo que desempeña	X	X	
Domicilio del trabajo	X	X	
Correo electrónico institucional	X	X	
Teléfono institucional	X	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
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)			

Área: DEPARTAMENTO DE SERVICIOS EDUCATIVOS

Nombre: SIXTO BURGUEÑO CASTAÑOS

Firma: _____

ISEJA

DEPARTAMENTO SERVICIOS EDUCATIVOS

"Este programa es público ajeno a cualquier partido político, queda prohibido el uso para fines distintos a los establecidos en el programa". Quién haga uso indebido de los recursos de este programa deberá ser denunciado/a y sancionado/a de acuerdo con la ley aplicable y ante la autoridad competente".

México 2021 Año de la Independencia

SINALOA
GOBIERNO DEL ESTADO

ISEJA
INSTITUTO SINALOENSE PARA LA EDUCACIÓN DE LOS JÓVENES Y ADULTOS

INVENTARIO DE DATOS PERSONALES SENSIBLES

DEPARTAMENTO DE SERVICIOS EDUCATIVOS

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 Área.

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			X
Información genética			X
Datos sobre vida sexual			
Preferencias sexuales			X
Practicas 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			
Otros datos personales (mencionar)			

Área: DEPARTAMENTO DE SERVICIOS EDUCATIVOS

Nombre: SIXTO BURGUEÑO CASTAÑOS

Firma: _____

ISEJA
DEPARTAMENTO
SERVICIOS
EDUCATIVOS

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

4.- Servidor Público Administrador del Departamento:

Cargo: Jefe del Departamento

Teléfono y Extensión: 667 715-0332 Ext 527

Funciones/Perfil: Cumplir con las funciones que correspondan al puesto de conformidad con el Decreto de Creación del ISEJA y realizar aquellas que le encomienden sus superiores jerárquicos.

Obligaciones: Entre otras, El seguimiento, acompañamiento pedagógico y la formación de figuras que participan en el proceso educativo, etc.

5.- Tipo de Soporte. - El soporte de los datos personales se encuentran en físico y de manera electrónica.

6.- Características del lugar donde se resguardan los sistemas de tratamiento de datos personales. – El Departamento Servicios Educativos del ISEJA, se encuentra en: Boulevard Ciudades Hermanas #665 oriente, colonia Antonio Rosales, C.P.80200, en Culiacán, Sinaloa.
Los archivos físicos se encuentran en una oficina con acceso restringido, solo se autoriza personal del Departamento y están depositados en archiveros con llave.

7.- Portabilidad de datos. – El Departamento Servicios Educativos, no cuenta con ningún formato estructurado para la portabilidad de datos.

8.- Transferencia de datos. - El Departamento Servicios Educativos, no transfiere los datos personales.

9.- Encargado de datos. - . El Departamento Servicios Educativos.

Departamento de Sistemas

1.- Fundamento Legal. – Capítulo cuarto, Artículo 12 del Decreto de Creación del Instituto Sinaloense Para la Educación de los Jóvenes y Adultos.

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

INVENTARIO DE DATOS PERSONALES GENERALES
DEPARTAMENTO DE SISTEMAS

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 Área.

Datos Personales Recabados	Existente	Necesario	No necesario
Datos de identificación y contacto			
Nombre	X		
Alias			X
Seudónimo			X
Sexo	X		
Estado Civil	X		
Registro Federal de Contribuyentes (RFC)	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		
Teléfono particular	X		
Teléfono celular personal	X		
Correo electrónico personal	X		
Firma autógrafa			X
Firma electrónica			X
Edad	X		
Fotografía	X		
Referencias personales			X
Escolaridad	X		
Número de seguridad social o análogo			X
Datos sobre características físicas			
Color de piel			X
Color de cabello			X
Señas particulares			X
Estatura			X
Peso			X
Cicatrices			X

Tipo de sangre			X
Datos biomédicos			
Datos Personales Recabados	**Existente**	**Necesario**	**No necesario**
Imagen de iris			**X**
Huella dactilar			X
Palma de la mano			X
ADN (Código genético)			X
Datos laborales			
Puesto o cargo que desempeña			X
Domicilio del trabajo			
Correo electrónico institucional			X
Teléfono institucional			
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,			X

datos de banda magnética, pin)			
Seguros			X
Afores			X
Datos sobre pasatiempos, entretenimientos y diversión			
Datos Personales Recabados	**Existente**	**Necesario**	**No necesario**
Pasatiempos			X
Aficiones			X
Deportes de practica			X
Juegos de su interés			X
Datos legales			
Situación jurídica de la persona (juicios, amparos, procesos administrativos, entre otros)			X
Otros datos personales (mencionar)			
Número de hijos(as)	X		
Lenguas	X		
Limitaciones físicas	x		

Área: SISTEMAS

Nombre: Juan Daniel Ochoa Flores

Firma:

INVENTARIO DE DATOS PERSONALES SENSIBLES

DEPARTAMENTO DE SISTEMAS

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 Área.

Datos personales recabados	Existente	Necesario	No necesario
Datos de identificación y contacto			
Posturas religiosas/ ideológicas/morales/filosóficas			X
Pertenencia a un partido/Posturas políticas			X
Pertenencia a un sindicato			X
Datos de Salud			
Estado de salud físico presente, pasado o futuro			X
Estado de salud mental presente, pasado o futuro			X
Información genética			X
Datos sobre vida sexual			
Preferencias sexuales			X
Practicas 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)			
Número de hijos(as)	X		
Lenguas	X		
Limitaciones físicas	X		

Área: Sistemas
Nombre: Juan Daniel Ochoa Flores
Firma:

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

4.- Servidor Público Administrador del Departamento:

Cargo: Jefe del Departamento

Teléfono y Extensión: 667 715-0332 Ext 504

Funciones/Perfil: Cumplir con las funciones que correspondan al puesto de conformidad con el Decreto de Creación del ISEJA y realizar aquellas que le encomienden sus superiores jerárquicos.

Obligaciones: Entre otras, seguimiento estadístico al proceso educativo, en virtud de una base de datos, así como el soporte técnico a las áreas administrativas en los diferentes procesos informáticos, etc.

5.- Tipo de Soporte. - El soporte de los datos personales se encuentran de manera electrónica.

6.- Características del lugar donde se resguardan los sistemas de tratamiento de datos personales. – El Departamento de Sistemas del ISEJA, se encuentra en: Boulevard Ciudades Hermanas #665 oriente, colonia Antonio Rosales, C.P.80200, en Culiacán, Sinaloa.

Los equipos de cómputo y servidor, se encuentran en una oficina con acceso restringido, solo se autoriza personal del Departamento y están depositados en archiveros con llave.

7.- Portabilidad de datos. – El Departamento de Sistemas, no cuenta con ningún formato estructurado para la portabilidad de datos.

8.- Transferencia de datos. - El Departamento de Sistemas, no transfiere los datos personales.

9.- Encargado de datos. - . El Departamento de Sistemas.

Unidad de Asuntos Jurídicos

1.- Fundamento Legal. – Capítulo cuarto, Artículo 12 del Decreto de Creación del Instituto Sinaloense Para la Educación de los Jóvenes y Adultos.

2.-Datos Personales que se encuentran en la Unidad:

SINALOA
GOBIERNO DEL ESTADO

ISEJA
INSTITUTO SINALOENSE PARA LA EDUCACIÓN DE LOS JÓVENES Y ADULTOS

INVENTARIO DE DATOS PERSONALES GENERALES

UNIDAD DE ASUNTOS JURÍDICOS

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 Área.

Datos Personales Recabados	Existente	Necesario	No 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 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	X	
Firma autógrafa	X	X	
Firma electrónica	X	X	
Edad	X	X	
Fotografía	X	X	
Referencias personales	X	X	
Escolaridad	X	X	
Número de seguridad social o análogo	X	X	

Datos sobre características físicas			
Color de piel	X		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 biomédicos			
Datos Personales Recabados	**Existente**	**Necesario**	**No necesario**
Imagen de iris	X		**X**
Huella dactilar	X		X
Palma de la mano	X		X
ADN (Código genético)			
Datos laborales			
Puesto o cargo que desempeña	X	X	
Domicilio del trabajo	X	X	
Correo electrónico institucional	X	X	
Teléfono institucional	X	X	
Referencia laborales	X	X	
Información generada durante los procedimientos de reclutamiento; selección y contratación	X	X	
Experiencia/Capacitación laboral	X	X	
Datos académicos			
Trayectoria educativa	X	X	
Títulos	X	X	
Cedula profesional	X	X	
Certificados	X	X	
Reconocimientos	X	X	
Datos migratorios			
Entrada al país			
Salida de país			
Tiempo de permanencia en el país			
Calidad migratoria			
Derechos de residencia			
Aseguramiento			

Repatriación			
Datos patrimoniales y/o financieros			
Bienes muebles			
Bienes inmuebles			
Información fiscal			
Historial crediticio/Buró de crédito			
Ingresos			
Egresos			
Cuentas bancarias			
Números de tarjetas de crédito			
Información adicional de tarjeta (fechas de vencimiento, códigos de seguridad, datos de banda magnética, pin)			
Seguros			
Afores			
Datos sobre pasatiempos, entretenimientos y diversión			
Datos Personales Recabados	**Existente**	**Necesario**	**No necesario**
Pasatiempos			
Aficiones			
Deportes de practica			
Juegos de su interés			
Datos legales			
Situación jurídica de la persona (juicios, amparos, procesos administrativos, entre otros)	X	X	
Otros datos personales (mencionar)			

Área: UNIDAD DE ASUNTOS JURÍDICOS
Nombre: DR. RUBÉN MIRANDA LÓPEZ

Firma: _____

INVENTARIO DE DATOS PERSONALES SENSIBLES

UNIDAD DE ASUNTOS JURÍDICOS

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 Área.

Datos personales recabados	Existente	Necesario	No necesario
Datos de identificación y contacto			
Posturas religiosas/ ideológicas/morales/filosóficas			
Pertenencia a un partido/Posturas políticas			
Pertenencia a un sindicato	X		X
Datos de Salud			
Estado de salud físico presente, pasado o futuro	X	X	
Estado de salud mental presente, pasado o futuro	X	X	
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	X		X
Datos Familiares			
Relaciones afectivas, familiares y conyugales	X	X	
Otros datos personales (mencionar)			

Área: UNIDAD DE ASUNTOS JURÍDICOS

Nombre: DR. RUBÉN MIRANDA LÓPEZ.

Firma: _____

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

4.- Servidor Público Administrador del Departamento:

Cargo: Responsable de la Unidad de Asuntos Jurídicos

Teléfono y Extensión: 667 715-0332 Ext 525

Funciones/Perfil: Cumplir con las funciones que correspondan al puesto de conformidad con el Decreto de Creación del ISEJA y realizar aquellas que le encomienden sus superiores jerárquicos.

Obligaciones: Entre otras, La representación Jurídica del Instituto, así como la asesoría permanente a las áreas administrativas del mismo. etc.

5.- Tipo de Soporte. - El soporte de los datos personales se encuentran en físico y de manera electrónica.

6.- Características del lugar donde se resguardan los sistemas de tratamiento de datos personales. – La Unidad de Asuntos Jurídicos del ISEJA, se encuentra en: Boulevard Ciudades Hermanas #665 oriente, colonia Antonio Rosales, C.P.80200, en Culiacán, Sinaloa.

Los archivos físicos se encuentran en una oficina con acceso restringido, solo se autoriza personal de la coordinación y están depositados en archiveros con llave.

7.- Portabilidad de datos. – La Unidad de Asuntos Jurídicos, no cuenta con ningún formato estructurado para la portabilidad de datos.

8.- Transferencia de datos. - La Unidad de Asuntos Jurídicos, no transfiere los datos personales.

9.- Encargado de datos. - . La Unidad de Asuntos Jurídicos.

Unidad de Transparencia

1.- Fundamento Legal. – Capítulo tercero, Artículo 67, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Sinaloa.

2.-Datos Personales que se encuentran en la Unidad:

SINALOA
GOBIERNO DEL ESTADO

ISEJA
INSTITUTO SINALOENSE PARA LA EDUCACIÓN DE LOS JÓVENES Y ADULTOS

INVENTARIO DE DATOS PERSONALES GENERALES

UNIDAD DE TRANSPARENCIA

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 Área.

Datos Personales Recabados	Existente	Necesario	No 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 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	X	
Firma autógrafa	X	X	
Firma electrónica	X	X	
Edad	X	X	
Fotografía	X	X	
Referencias personales	X	X	
Escolaridad	X	X	
Número de seguridad social o análogo	X	X	

Datos sobre características físicas			
Color de piel	X		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 biomédicos			
Datos Personales Recabados	**Existente**	**Necesario**	**No necesario**
Imagen de iris	X		**X**
Huella dactilar	X		X
Palma de la mano	X		X
ADN (Código genético)			
Datos laborales			
Puesto o cargo que desempeña	X	X	
Domicilio del trabajo	X	X	
Correo electrónico institucional	X	X	
Teléfono institucional	X	X	
Referencia laborales	X	X	
Información generada durante los procedimientos de reclutamiento; selección y contratación	X	X	
Experiencia/Capacitación laboral	X	X	
Datos académicos			
Trayectoria educativa	X	X	
Títulos	X	X	
Cedula profesional	X	X	
Certificados	X	X	
Reconocimientos	X	X	
Datos migratorios			
Entrada al país			
Salida de país			
Tiempo de permanencia en el país			
Calidad migratoria			
Derechos de residencia			
Aseguramiento			

"Este programa es público ajeno a cualquier partido político, queda prohibido el uso para fines distintos a los establecidos en el programa". Quién haga uso indebido de los recursos de este programa deberá ser denunciado/a y sancionado/a de acuerdo con la ley aplicable y ante la autoridad competente".

2022 Ricardo Flores Magón

Repatriación			
Datos patrimoniales y/o financieros			
Bienes muebles			
Bienes inmuebles			
Información fiscal			
Historial crediticio/Buró de crédito			
Ingresos			
Egresos			
Cuentas bancarias			
Números de tarjetas de crédito			
Información adicional de tarjeta (fechas de vencimiento, códigos de seguridad, datos de banda magnética, pin)			
Seguros			
Afores			
Datos sobre pasatiempos, entretenimientos y diversión			
Datos Personales Recabados	**Existente**	**Necesario**	**No necesario**
Pasatiempos			
Aficiones			
Deportes de practica			
Juegos de su interés			
Datos legales			
Situación jurídica de la persona (juicios, amparos, procesos administrativos, entre otros)	X	X	
Otros datos personales (mencionar)			

Área: UNIDAD DE TRANSPARENCIA
Nombre: DR. RUBÉN ANTONIO GONZÁLEZ FRANCO

Firma: _____

"Este programa es público ajeno a cualquier partido político, queda prohibido el uso para fines distintos a los establecidos en el programa". Quién haga uso indebido de los recursos de este programa deberá ser denunciado/a y sancionado/a de acuerdo con la ley aplicable y ante la autoridad competente".

INVENTARIO DE DATOS PERSONALES SENSIBLES

UNIDAD DE TRANSPARENCIA

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 Área.

Datos personales recabados	Existente	Necesario	No necesario
Datos de identificación y contacto			
Posturas religiosas/ ideológicas/morales/filosóficas			
Pertenencia a un partido/Posturas políticas			
Pertenencia a un sindicato	X		X
Datos de Salud			
Estado de salud físico presente, pasado o futuro	X	X	
Estado de salud mental presente, pasado o futuro	X	X	
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	X		X
Datos Familiares			
Relaciones afectivas, familiares y conyugales	X	X	
Otros datos personales (mencionar)			

Área: UNIDAD DE TRANSPARENCIA

Nombre: DR. RUBÉN ANTONIO GONZÁLEZ FRANCO.

Firma: _____

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

4.- Servidor Público Administrador de la Unidad:

Cargo: Responsable de la Unidad de Transparencia.

Teléfono y Extensión: 667 715-0332 Ext 525

Funciones/Perfil: Cumplir con las funciones que correspondan a la responsabilidad conferida 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, recibir y dar trámite a las solicitudes de acceso a la información, así como el rubro de protección de datos personales, etc.

5.- Tipo de Soporte. - El soporte de los datos personales se encuentran en físico y de manera electrónica.

6.- Características del lugar donde se resguardan los sistemas de tratamiento de datos personales. – La Unidad de Transparencia del ISEJA, se encuentra en: Boulevard Ciudades Hermanas #665 oriente, colonia Antonio Rosales, C.P.80200, en Culiacán, Sinaloa.

Los archivos físicos se encuentran en una oficina con acceso restringido, solo se autoriza personal de la unidad y están depositados en archiveros con llave.

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. - . La Unidad de Transparencia.

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 abordarán 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, el ISEJA, cuenta con las siguientes:

De Tipo Físico:

a) Prevenir el acceso no autorizado al perímetro del ISEJA, sus instalaciones físicas, áreas críticas, recursos e información;
   Para lo anterior, el ISEJA, cuenta con personal de vigilancia que tiene por objeto la vigilancia, protección a instalaciones, bienes y personas en las oficinas que ocupa el ISEJA.

b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas del ISEJA, 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 ISEJA, 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 edificio 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 Jefe 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 ISEJA 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.

I. 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 acabo 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 algún otro Departamento.
Terceros	Si se refiere a algún ente externo al ISEJA.

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

IX. Análisis de Brecha.

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

X. Plan de Trabajo.

Una vez realizado en análisis de riesgo y el análisis de brecha, cada Área 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 digito: Empieza con una letra Mayúscula que corresponde a una Coordinación, Departamento o Unidad del ISEJA.

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

Tercer digito: 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 digito: 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.

Coordinación Regional.

1. Medidas de Seguridad actuales:

TIPO	CONTROL/MECANISMO	ID	MEDIDAS ACTUALES
ADMINISTRATIVAS	Políticas interna de protección de datos personales.	C1.1.1	
	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.		
FÍSICAS	Prevenir el Acceso no autorizado a la oficina donde se tienen resguardados los datos personales.	C2.1.1	
	Los expedientes deben de estar en archiveros con llave.	C2.1.2	
	No dejar expedientes sobre el escritorio si no se están utilizando.	C2.1.3	
TECNOLÓGICAS	Para ingresar al sistema se necesita proporcionar usuario y contraseña.	C3.1.1	
	El equipo de cómputo se encuentra protegido con acceso restringido a la red del Instituto, por antivirus y Firewalls.	C3.1.2	
	Los Sistemas y plataformas utilizadas, tiene medidas de seguridad que limitan el acceso a sus bases de datos.	C3.1.3	

2. Análisis de Riegos:

Medidas de seguridad actuales	ID	Riesgo/amenaza	Factor de Riesgo	Clasificación del Riesgo	Control del Factor	Valoración de Riesgo	
						Impacto/probabilidad de que ocurra	valor
C1.1.1	C1.2.1						
C2.1.1	C2.2.1						
C2.1.2	C2.2.2						
C2.1.3	C2.2.3						

3. Análisis de Brecha:

Medidas de seguridad actuales	Riesgos	ID	Identificación de la Brecha
C1.1.1	C1.2.1	C1.3.1	
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	

4.- Plan de Trabajo:

Brecha que se Atiende	Planificación				Evidencia/Entregable
	ID	Actividad	Responsable	Fecha Tentativa	
C1.3.1	C1.4.1				
C2.3.1	C2.4.1				
C2.3.2	C2.4.2				
C2.3.3	C2.4.3				

Departamento de Administración y Finanzas

1. Medidas de Seguridad actuales:

TIPO	CONTROL/MECANISMO	ID	MEDIDAS ACTUALES
ADMINISTRATIVAS	Políticas interna de protección de datos personales.	F1.1.1	
	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.		
FÍSICAS	Prevenir el Acceso no autorizado a la oficina donde se tienen resguardados los datos personales.	F2.1.1	
	Los expedientes deben de estar en archiveros con llave.	F2.1.2	
	No dejar expedientes sobre el escritorio si no se están utilizando.	F2.1.3	
TECNOLÓGICAS	Para ingresar al sistema se necesita proporcionar usuario y contraseña.	F3.1.1	
	El equipo de cómputo se encuentra protegido con acceso restringido a la red del Instituto, por antivirus y Firewalls.	F3.1.2	
	Los Sistemas y plataformas utilizadas, tiene medidas de seguridad que limitan el acceso a sus bases de datos.	F3.1.3	

2. Análisis de Riegos:

Medidas de seguridad actuales	ID	Riesgo/amenaza	Factor de Riesgo	Clasificación del Riesgo	Control del Factor	Valoración de Riesgo	
						Impacto/probabilidades que ocurra	valor
F1.1.1	F1.2.1						
F2.1.1	F2.2.1						
F2.1.2	F2.2.2						
F2.1.3	F2.2.3						
F3.1.1	F3.2.1						
F3.1.2	F3.2.2						
F3.1.3	F3.2.3						

3. Análisis de Brecha:

Medidas de seguridad actuales	Riesgos	ID	Identificación de la Brecha
F1.1.1	F1.2.1	F1.3.1	
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	
F3.1.1	F3.2.1	F3.3.1	
F3.1.2	F3.2.2	F3.3.2	
F3.1.3	F3.2.3	F3.3.2	

4.- Plan de Trabajo:

Brecha que se Atiende	Planificación				Evidencia/Entregable
	ID	Actividad	Responsable	Fecha Tentativa	
F1.3.1	F1.4.1				
F2.3.1	F2.4.1				
F2.3.2	F2.4.2				
F2.3.3	F2.4.3				
F3.3.1	F3.4.1				
F3.3.2	F3.4.2				
F3.3.2	F3.4.3				

Departamento de Planeación y Seguimiento operativo

1. Medidas de Seguridad actuales:

TIPO	CONTROL/MECANISMO	ID	MEDIDAS ACTUALES
ADMINISTRATIVAS	Políticas internas de protección de datos personales.	P1.1.1	
	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.		
FÍSICAS	Prevenir el Acceso no autorizado a la oficina donde se tienen resguardados los datos personales.	P2.1.1	
	Los expedientes deben de estar en archiveros con llave.	P2.1.2	
	No dejar documentación sobre el escritorio si no se están utilizando.	P2.1.3	
TECNOLÓGICAS	Para ingresar al sistema se necesita proporcionar usuario y contraseña.	P3.1.1	
	El equipo de cómputo se encuentra protegido con acceso restringido a la red del Instituto, por antivirus y Firewalls.	P3.1.2	
	Los Sistemas y plataformas utilizadas, tiene medidas de seguridad que limitan el acceso a sus bases de datos.	P3.1.3	

2. Análisis de Riegos:

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
P1.1.1	P1.2.1						
P2.1.1	P2.2.1						
P2.1.2	P2.2.2						
P2.1.3	P2.2.3						

3. Análisis de Brecha:

Medidas de seguridad actuales	Riesgos	ID	Identificación de la Brecha
P1.1.1	P1.2.1	P1.3.1	
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	

4.- Plan de Trabajo:

Brecha que se Atiende	Planificación				Evidencia/Entregable
	ID	Actividad	Responsable	Fecha Tentativa	
P1.3.1	P1.4.1				
P2.3.1	P2.4.1				
P2.3.2	P2.4.2				
P2.3.3	P2.4.3				

Departamento de Acreditación

1. Medidas de Seguridad actuales:

TIPO	CONTROL/MECANISMO	ID	MEDIDAS ACTUALES
ADMINISTRATIVAS	Políticas internas 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.		
FÍSICAS	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 Riegos:

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						
A3.1.1	A3.2.1						
A3.1.2	A3.2.2						

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	
A3.1.1	A3.2.1	A3.3.1	
A3.1.2	A3.2.2	A3.3.2	

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				
A3.3.1	A3.4.1				
A3.3.2	A3.4.2				

Departamento de Servicios Educativos

1. Medidas de Seguridad actuales:

TIPO	CONTROL/MECANISMO	ID	MEDIDAS ACTUALES
ADMINISTRATIVAS	Políticas interna de protección de datos personales.	E1.1.1	
	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.		
FÍSICAS	Prevenir el Acceso no autorizado a la oficina donde se tienen resguardados los datos personales.	E2.1.1	
	Los expedientes deben de estar en archiveros con llave.	E2.1.2	
	No dejar expedientes sobre el escritorio si no se están utilizando.	E2.1.3	
TECNOLÓGICAS	Para ingresar al equipo de cómputo se necesita proporcionar usuario y contraseña.	E3.1.1	
	El equipo de cómputo se encuentra protegido con acceso restringido a la red de gobierno, por antivirus y Firewalls.	E3.1.2	

2. Análisis de Riegos:

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
E1.1.1	E1.2.1						
E2.1.1	E2.2.1						
E2.1.2	E2.2.2						
E2.1.3	E2.2.3						
E3.1.1	E3.2.1						
E3.1.2	E3.2.2						

3. Análisis de Brecha:

Medidas de seguridad actuales	Riesgos	ID	Identificación de la Brecha
E1.1.1	E1.2.1	E1.3.1	
E2.1.1	E2.2.1	E2.3.1	
E2.1.2	E2.2.2	E2.3.2	
E2.1.3	E2.2.3	E2.3.3	
E3.1.1	E3.2.1	E3.3.1	
E3.1.2	E3.2.2	E3.3.2	

4.- Plan de Trabajo:

Brecha que se Atiende	Planificación				Evidencia/Entregable
	ID	Actividad	Responsable	Fecha Tentativa	
E1.3.1	E1.4.1				
E2.3.1	E2.4.1				
E2.3.2	E2.4.2				
E2.3.3	E2.4.3				
E3.3.1	E3.4.1				
E3.3.2	E3.4.2				

Departamento de Sistemas.

1. Medidas de Seguridad actuales:

TIPO	CONTROL/MECANISMO	ID	MEDIDAS ACTUALES
ADMINISTRATIVAS	Políticas internas de protección de datos personales.	S1.1.1	
	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.		
FÍSICAS	Prevenir el Acceso no autorizado a la oficina donde se tienen resguardados los datos personales.	S2.1.1	
	Los archivos deben de estar protegidos mediante contraseñas.	S2.1.2	
	No dejar dispositivos sobre el escritorio si no se están utilizando.	S2.1.3	
TECNOLÓGICAS	Para ingresar al equipo de cómputo se necesita proporcionar usuario y contraseña.	S3.1.1	
	El equipo de cómputo se encuentra protegido con acceso restringido a la red Institucional, por antivirus y Firewalls.	S3.1.2	

2. Análisis de Riegos:

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
SF1.1.1	S1.2.1						
S2.1.1	S2.2.1						
S2.1.2	S2.2.2						
S2.1.3	S2.2.3						
S3.1.1	S3.2.1						
S3.1.2	S3.2.2						

3. Análisis de Brecha:

Medidas de seguridad actuales	Riesgos	ID	Identificación de la Brecha
S1.1.1	S1.2.1	S1.3.1	
S2.1.1	S2.2.1	S2.3.1	
S2.1.2	S2.2.2	S2.3.2	
S2.1.3	S2.2.3	S2.3.3	
S3.1.1	S3.2.1	S3.3.1	
S3.1.2	S3.2.2	S3.3.2	

4.- Plan de Trabajo:

Brecha que se Atiende	Planificación				Evidencia/Entregable
	ID	Actividad	Responsable	Fecha Tentativa	
S1.3.1	F1.4.1				
S2.3.1	F2.4.1				
S2.3.2	S2.4.2				
S2.3.3	S2.4.3				
S3.3.1	S3.4.1				
S3.3.2	S3.4.2				

Unidad de Asuntos Jurídicos

1. Medidas de Seguridad actuales:

TIPO	CONTROL/MECANISMO	ID	MEDIDAS ACTUALES
ADMINISTRATIVAS	Políticas internas de protección de datos personales.	J1.1.1	
	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.		
FÍSICAS	Prevenir el Acceso no autorizado a la oficina donde se tienen resguardados los datos personales.	J2.1.1	
	Los expedientes deben de estar en archiveros con llave.	J2.1.2	
	No dejar expedientes sobre el escritorio si no se están utilizando.	J2.1.3	
TECNOLÓGICAS	Para ingresar al equipo de cómputo se necesita proporcionar usuario y contraseña.	J3.1.1	
	El equipo de cómputo se encuentra protegido con acceso restringido a la red de gobierno, por antivirus y Firewalls.	J3.1.2	

2. Análisis de Riegos:

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
J1.1.1	J1.2.1						
J2.1.1	J2.2.1						
J2.1.2	J2.2.2						
J2.1.3	J2.2.3						
J3.1.1	J3.2.1						
J3.1.2	J3.2.2						

3. Análisis de Brecha:

Medidas de seguridad actuales	Riesgos	ID	Identificación de la Brecha
J1.1.1	J1.2.1	J1.3.1	
J2.1.1	J2.2.1	J2.3.1	
J2.1.2	J2.2.2	J2.3.2	
J2.1.3	J2.2.3	J2.3.3	
J3.1.1	J3.2.1	J3.3.1	
J3.1.2	J3.2.2	J3.3.2	

4.- Plan de Trabajo:

Brecha que se Atiende	Planificación				Evidencia/Entregable
	ID	Actividad	Responsable	Fecha Tentativa	
J1.3.1	J1.4.1				
J2.3.1	J2.4.1				
J2.3.2	J2.4.2				
J2.3.3	J2.4.3				
J3.3.1	J3.4.1				
J3.3.2	J3.4.2				

Unidad de Transparencia

1. Medidas de Seguridad actuales:

TIPO	CONTROL/MECANISMO	ID	MEDIDAS ACTUALES
ADMINISTRATIVAS	Políticas internas de protección de datos personales.	T1.1.1	
	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.		
FÍSICAS	Prevenir el Acceso no autorizado a la oficina donde se tienen resguardados los datos personales.	T2.1.1	
	Los expedientes deben de estar en archiveros con llave.	T2.1.2	
	No dejar expedientes sobre el escritorio si no se están utilizando.	T2.1.3	
TECNOLÓGICAS	Para ingresar al equipo de cómputo se necesita proporcionar usuario y contraseña.	T3.1.1	
	El equipo de cómputo se encuentra protegido con acceso restringido a la red de gobierno, por antivirus y Firewalls.	T3.1.2	

2. Análisis de Riegos:

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
T1.1.1	T1.2.1						
T2.1.1	T2.2.1						
T2.1.2	T2.2.2						
T2.1.3	T2.2.3						
T3.1.1	T3.2.1						
T3.1.2	T3.2.2						

3. Análisis de Brecha:

Medidas de seguridad actuales	Riesgos	ID	Identificación de la Brecha
T1.1.1	T1.2.1	T1.3.1	
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	
T3.1.1	T3.2.1	T3.3.1	
T3.1.2	T3.2.2	T3.3.2	

4.- Plan de Trabajo:

Brecha que se Atiende	Planificación				Evidencia/Entregable
	ID	Actividad	Responsable	Fecha Tentativa	
T1.3.1	T1.4.1				
T2.3.1	T2.4.1				
T2.3.2	T2.4.2				
T2.3.3	T2.4.3				
T3.3.1	T3.4.1				
T3.3.2	T3.4.2				

XII. Mecanismos de Monitoreo.

En términos de lo dispuesto por la LPDPPSOES, para la protección de datos personales, el ISEJA 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 Departamento, se estará solicitando a cada Departamento envié a la Unidad de Transparencia, copia de la evidencia que sustente las actividades realizadas.
Posteriormente, en la actualización anual que corresponda, se estará trabajando con las titulares de cada departamento, respecto a la efectividad de las medidas de seguridad implementadas, con la finalidad de evitar alteración, perdida o acceso no autorizado a los datos personales objeto de tratamiento.

XIII. Programa General de Capacitación.

Entre las atribuciones de la Unidad de Transparencia, está la de coordinar la capacitación continua y especializada del personal del ISEJA en materia de su competencia.
Derivado de lo anterior, la Unidad de Transparencia, capacita a todos los funcionarios públicos mediante el taller “Protección de Datos Personales, Medidas de Seguridad y Avisos de Privacidad”, particularmente se imparte este taller a todo nuevo servidor público que tenga entre sus actividades el tratamiento y resguardo de los datos personales.

XIV. Actualizaciones

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

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

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

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

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

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

Aprobación.

El presente documento fue aprobado por unanimidad de los integrantes del Comité de Transparencia del Instituto Sinaloense para la Educación de los Jóvenes y Adultos, en la Primera Sesión Ordinaria efectuada el día 02 de febrero de 2022.