ANEXO A LA VERSION PÚBLICA DEL DOCUMENTO DE SEGURIDAD DE CEAIP

INFORMACIÓN TESTADA POR SER CLASIFICADA COMO RESERVADA	PÁGINAS	FUNDAMENTO LEGAL	MOTIVACIÓN APLICABLE A
Sitios de Resguardo	8,10,12,14,19,21, 23,25,27,28,30,32, 34,36,37,40,42,44, 46,48,49,51,53,54, 56,58,59,61,63,65, 67 y 70.	Artículo 162 fracción IV, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Sinaloa.	Con la publicidad integra de la información objeto de la solicitud, se pone en riesgo la vida y seguridad de los servidores públicos de esta Comisión, proveedores de servicios, prestadores de servicios y usuarios de la Plataforma Nacional de Transparencia en Sinaloa, ya que al dar a conocer las especificaciones o características de las medidas de seguridad técnicas y físicas adoptadas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales, los sitios de resguardo de los datos personales, el análisis de riesgos, el análisis de brecha y el plan de trabajo, la cual es información que refleja las prácticas de seguridad de los datos personales, los niveles de riesgos identificados y las vulnerabilidades de dichos sistemas, se expondrían a la comisión de diversos delitos como asaltos, extorsiones, suplantación de identidad, o secuestros por mencionar algunos, tomando en consideración que los referidos sistemas albergan datos personales identificativos, causal prevista en la fracción IV del artículo 162 de la ley de transparencia estatal. En ese orden de ideas, se destaca que la reserva aprobada por el Comité de Transparencia, busca proteger la información y las bases de datos personales, evitando exponerlas a un ataque de pudiera conseguir vulnerarlas para beneficiarse de los datos personales contenidos en ellas, ya que al exponerse dicha información se pone en riesgo la vida y seguridad de los servidores públicos, proveedores de servicios, prestadores de servicios y usuarios de la Plataforma Nacional de Transparencia.
Especificaciones o características de las medidas de seguridad técnicas y físicas adoptadas	75, 76 y 77		
Análisis de riesgos	85,86,87,88,89,90 y 91.		
Análisis de brecha	95 y 96		
Plan de trabajo	96		

2022

DOCUMENTO DE SEGURIDAD

Comisión Estatal para el Acceso a la Información Pública

Este documento contiene las medidas de seguridad administrativas, físicas y técnicas con las que cuenta la CEAIP para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee cada una de las áreas.

COMITÉ DE TRANSPARENCIA

Primera versión

CONTENIDO

1. **Presentación**..... 2
2. **Glosario**.....3
3. **Inventario de datos personales y de los sistemas de tratamiento por área administrativa**.....6

   3.1 Dirección de Administración.....6
   3.2 Órgano Interno de Control.....13
   3.3 Unidad de Transparencia.....20
   3.4 Dirección Jurídica Consultiva.....28
   3.5 Secretaría Ejecutiva..... 33
   3.6 Unidad de Gobierno Abierto..... 35
   3.7 Dirección de Capacitación.....39
   3.8 Departamento de Comunicación..... 47
   3.9 Coordinación de Sistemas Informáticos..... 51
   3.10 Coordinación Estatal de la Plataforma Nacional de Transparencia.....62
   3.11 Ponencias.....66
   3.12 Coordinación de Archivos.....68
   3.13 Dirección de Verificación y Seguimiento.....71
   3.14 Dirección de Datos Personales.....71
4. **Medidas de Seguridad**.....73
   4.1 Medidas de seguridad administrativas 73
   4.2 Medidas de seguridad físicas..... 75
   4.3 Medidas de seguridad técnicas..... 79
5. **Análisis de riesgos** 84
6. **Análisis de brecha**..... 98
7. **Plan de trabajo**..... 104
8. **Mecanismos de monitoreo y revisión de las medidas de seguridad**.....108
9. **Programa general de capacitación** 108
10. **Actualización del documento de seguridad**..... 109
11. **Directorio**..... 110
12. **Anexo 1** (Relación de servidores públicos que tienen acceso a los sistemas de datos personales) 112
13. **Anexo 2** (Encargados de datos personales) 116
14. **Anexo 3** (Control de versiones y/o actualizaciones) 117

1. PRESENTACIÓN

Con la publicación de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) en enero de 2017, se establecieron las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales en posesión de sujetos obligados.

De manera armónica, en el ámbito local, dichas bases, principios y procedimientos quedaron establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Sinaloa, misma que fue publicada en julio de 2017.

Ambas legislaciones prevén la necesidad de realizar diversas actividades interrelacionadas para establecer y mantener medidas de seguridad encaminadas a la protección de los datos personales, como la creación de políticas internas para su gestión y tratamiento; la definición de funciones y obligaciones del personal involucrado en el tratamiento; la elaboración de un inventario de datos personales y de los sistemas de tratamiento; la realización de un análisis de riesgo considerando amenazas y vulnerabilidades existentes y recursos para su tratamiento; la realización de un análisis de brecha que compare medidas de seguridad, así como la elaboración de un plan de trabajo para implementar las faltantes; el monitoreo y revisión de las medidas de seguridad; incluido el diseño y aplicación de diferentes niveles de capacitación en la materia.

Asimismo, la propia legislación establece la necesidad de que las medidas de seguridad se encuentren debidamente documentadas y en particular prevé la elaboración de un documento de seguridad, el cual es un instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee y el cual permite conocer las áreas de oportunidad y las líneas de acción para subsanar y atender los riesgos identificados en materia de seguridad de datos personales.

En cumplimiento a lo anterior, la Dirección de Datos Personales elaboró el presente documento de seguridad mismo que fue revisado y aprobado por el Comité de Transparencia como autoridad máxima en materia de protección de datos personales al interior de la CEAIP, documento que es de observancia obligatoria para las y los servidores públicos de ésta, que realicen algún tipo de tratamiento de datos personales, incluyendo, en su caso, a encargados.

2. GLOSARIO

Área administrativa: Unidades que conforman la estructura orgánica de la CEAIP, cuyos titulares de cada una de las áreas figuran como responsables del tratamiento de datos personales en particular.

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

CEAIP o Comisión: Comisión Estatal para el Acceso a la Información Pública.

Documento de seguridad: Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

Cómputo en la nube: Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente.

DMZ: Red aislada que se encuentra dentro de la red interna de la Comisión. En ella se encuentran ubicados exclusivamente todos los recursos que deben ser accesibles desde Internet, como el servidor web (portal institucional) o de correo electrónico.

Encargado: Persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable.

Firewall: Dispositivo de seguridad cuya función principal es la de **filtrar el tráfico** de red entrante y saliente por medio de una serie de reglas, que permitirán su paso o rechazo.

Hardware: Conjunto de componentes físicos de los que está hecho el equipo de cómputo.

Ley General: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

LPDPPSOES: Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estados de Sinaloa.

Ley de Transparencia o LTAIPES: Ley de Transparencia y Acceso a la Información Pública del Estado de Sinaloa.

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten garantizar la protección, confidencialidad, disponibilidad e integridad de los datos personales.

Medidas de seguridad administrativas: Políticas y procedimiento para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional.

Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.

Medidas de seguridad técnicas: 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 recursos involucrados en su tratamiento.

Reglamento Interior: Reglamento Interior de la Comisión Estatal para el Acceso a la Información Pública.

Respaldo o Backup: Copia electrónica de la información que se genera, utiliza y actualiza a lo largo del tiempo; también este término se emplea

para referirse a las copias de seguridad que se llevan a cabo en los sistemas de información, bases de datos, software de aplicación, sistemas operativos, utilerías, entre otros. El objetivo de un respaldo es garantizar la recuperación de la información, en caso de que haya sido eliminada, dañada o alterada al presentarse alguna contingencia.

Sistema de Datos Personales: Conjunto organizado de archivos, registros, ficheros, bases o banco de datos personales de los entes públicos, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso.

Software: Conjunto de programas o aplicaciones, instrucciones y reglas informáticas que hacen posible el funcionamiento del equipo de cómputo.

Tercero: Persona física o jurídica colectiva, autoridad pública, servicio u organismo distinto de la o el titular, responsable, encargado, usuaria o usuario, destinataria o destinatario y las personas autorizadas para tratar los datos personales.

Titular: Persona física a quien pertenecen los datos personales.

Transferencia: Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, responsable o encargado.

Tratamiento: De manera enunciativa mas no limitativa cualquier operación o conjunto de operaciones efectuadas mediante procedimiento manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de los datos personales.

Usuarias o Usuarios: Servidoras y servidores públicos o personas físicas autorizadas para tratar los datos personales, distintos al responsable, al encargado y al administrador de los datos.

3. INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO POR ÁREA ADMINISTRATIVA

El inventario es la descripción de cada base o sistema de tratamiento de datos personales, se indican cuáles se recaban, con qué finalidad y mediante qué forma se obtienen, el fundamento legal que faculta al área administrativa para el tratamiento, los medios de almacenamiento, sitios de resguardo, si existen encargados que actúen a cuenta y nombre de la Comisión y, el servidor público que administre la base o sistema de tratamiento, así como los subordinados que tienen acceso a las mismas, de acuerdo a lo dispuesto por el artículo 46, fracciones I y II de la Ley.

A continuación, se precisa cada uno de los sistemas de tratamiento de datos personales existentes por cada una de las áreas administrativas de la CEAIP:

3.1 DIRECCIÓN DE ADMINISTRACIÓN

A.1.- Sistema de Expedientes del personal

1.- Servidor público responsable del sistema o base de tratamiento.

Titular de la Dirección de Administración.

2.- Funciones y obligaciones de las personas que tratan los datos personales.

Esta base de datos o sistema de tratamiento es con el fin de integrar los datos personales de los servidores públicos adscritos a esta Comisión a un expediente y posteriormente tener acceso a los mismos para su consulta, así como realizar los trámites correspondientes ante la institución bancaria para la apertura de la cuenta de nómina y además, poder cumplir con los pagos de impuestos y aportaciones que resulten aplicables.

La Dirección de Administración tiene funciones para realizar el tratamiento de datos personales, con fundamento en los artículos 48 fracción V del Reglamento Interior; 99 fracción III de la Ley del Impuesto Sobre la Renta; artículos 5 A, fracción XV y 15, fracción III de la Ley del Seguro Social; y, 17 de la Ley de Hacienda del Estado de Sinaloa.

3.- Datos personales que se recaban y su finalidad.

DATO PERSONAL	FINALIDAD
Nombre	**Principal:** Todos estos datos personales se utilizan para la integración del expediente personal, trámites administrativos y consultas.
Edad	
Sexo	
Estado civil	
Domicilio	
Escolaridad (con el respectivo documento comprobatorio)	
Nacionalidad	
Número telefónico particular	
Número telefónico celular	
Correo electrónico particular	
Numero de seguridad social	
Número de cuenta bancaria	
Beneficiarios de las cuentas bancarias.	
Registro Federal de Contribuyentes (RFC).	
Deducciones personales (como préstamos, pensiones de alimentos, etc.).	
Clave Única de Registro de Población (CURP).	
Estado de salud (para aquellos casos en los que se presentan justificantes médicos e incapacidades médicas).	

4.- Forma de obtención y medios de almacenamiento.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO

Directa	**Físico y Electrónico**

5.- Sitios de resguardo.

[redacted]

6.- Servidores públicos que tienen acceso a los sistemas de datos personales.

Titular de la Dirección de Administración y Analistas contables adscritos al área, así como la Coordinación de Archivos, una vez que se realiza la transferencia primaria al archivo de concentración para su resguardo.

7.- Encargado.

Proveedor/Tercero	No aplica
Actividad	No aplica
Relación	No aplica
Instrumento jurídico que formaliza la prestación del servicio	No aplica

8.- Transferencias a terceros que se realizan.

Se realizan transferencias de datos al Instituto Mexicano del Seguro Social (IMSS), Institución Bancaria, Servicio de Administración Tributaria del Estado de Sinaloa (SATES) y Servicio de Administración Tributaria (SAT).

9. Control archivístico.

Serie documental: CEAIP.05.00.04.00

Plazos de conservación: Archivo de Trámite / 2 años – Archivo de Concentración / 10 años.

A.2.- Sistema de procedimientos de contratación y pagos a proveedores.

1.- Servidor público responsable del sistema o base de tratamiento.

Titular de la Dirección de Administración.

2.- Funciones y obligaciones de las personas que tratan los datos personales.

Esta base de datos o sistema de tratamiento es para integrar el procedimiento de contratación, elaboración de contrato y/o pedido de bienes o suministros, las pólizas contables con la documentación comprobatoria del gasto, así como la realización de los pagos y transferencias que correspondan a la Comisión.

La Dirección de Administración de la CEAIP cuenta con facultades y obligaciones para tratar datos personales, esto con fundamento en el artículo 48, fracciones XII, XIII, XV y XVI del Reglamento Interior de esta Comisión.

3.- Datos personales que se recaban y su finalidad.

DATO PERSONAL/CONFIDENCIAL	FINALIDAD
Nombre	**Principal:** Los datos personales recabados serán protegidos, incorporados y tratados en los expedientes administrativos que se ubicarán en la Dirección de Administración, dicha información tiene como finalidad integrar el procedimiento de contratación, elaboración del contrato y/o pedido, las pólizas contables con la documentación comprobatoria del gasto, así como la realización de los pagos y transferencias que correspondan a la Comisión.
Nacionalidad	
Domicilio Fiscal	
Teléfono	
Correo electrónico comercial	
Registro Federal de Contribuyentes (RFC)	
Firma autógrafa	
Identificación oficial	
Número de cuenta	
Clave interbancaria	
Constancia de situación fiscal	

4.- Forma de obtención y medios de almacenamiento.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directa	**Físico y electrónico**

5. - Sitios de resguardo.

[redacted]

6.- Servidores públicos que tienen acceso a los sistemas de datos personales.

Titular de la Dirección de Administración; Jefe de Bienes y Suministros; Analistas contables adscritos al área y la Coordinación de Archivos, una vez que se realiza la trasferencia primaria al Archivo de Concentración para su resguardo.

7.- Encargado.

Proveedor/Tercero	No aplica.
Actividad	
Relación	
Instrumento jurídico que formaliza la prestación del servicio	

8.- Transferencias que se realizan.

No se realizan transferencias a terceros.

9.Control archivístico.

Series documentales: CEAIP.05.00.08.02 (pólizas de egreso)
CEAIP.05.00.08.03 (pólizas de diario)

Plazos de conservación: Archivo de Trámite / 2 años – Archivo de Concentración / 8 años.

A.3.- Sistema de Recibos de Nómina

1.- Servidor público responsable del sistema o base de tratamiento.

Titular de la Dirección de Administración y analista contable.

2.- Funciones y obligaciones de las personas que tratan los datos personales.

Esta base de datos o sistema de tratamiento es con el fin de registrar y realizar el pago correspondiente de las percepciones de los servidores públicos de la CEAIP, así como enterar las cuotas e impuestos aplicables.

La Dirección de Administración cuenta con facultades y obligaciones para tratar datos personales con fundamento en los artículos 5, fracción XV, 15, fracción III y 38 de la Ley del Seguro Social; 1 y 94 de la Ley del Impuesto Sobre la Renta; 17, 17 Bis, 18, 19 y 21 de la Ley de Hacienda del Estado de Sinaloa; 28, fracción XXXVIII y 48, fracciones V, VI, XV y XVI del Reglamento Interior de la Comisión.

3.- Datos personales que se recaban y su finalidad.

DATO PERSONAL	FINALIDAD
Nombre	**Principal:** Registrar y realizar el pago correspondiente de las percepciones de los servidores públicos de la CEAIP.
Registro Federal de Contribuyentes (RFC)	
Clave Única de Registro de Población (CURP)	
Número de seguridad social	
Número de cuenta bancaria	
Deducciones personales (como préstamos, pensiones de alimentos, etc.)	

4.- Forma de obtención y medios de almacenamiento.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directa	**Físico y electrónico**

5.- Sitios de resguardo.

[redacted]

6.- Servidores públicos que tienen acceso a los sistemas de datos personales.

Titular de la Dirección de Administración, Analista adscrito al área y la Coordinación de Archivos, una vez que se realiza la trasferencia primaria al Archivo de Concentración para su resguardo.

7.- Encargado.

Proveedor/Tercero	Despacho contable externo autorizado
Actividad	Auditoría de Estados Financieros
Relación	Contratación de Servicios Profesionales
Instrumento jurídico que formaliza la prestación del servicio	Contrato de prestación de servicios profesionales

8.- Transferencias que se realizan.

Se realizan transferencias de datos a la Auditoria Superior de la Federación (ASF) y Auditoria Superior del Estado (ASE) para efecto de que puedan realizar la auditoría externa que mandata la Ley.

9.- Control archivístico.

Serie documental: CEAIP.05.00.08.05

Plazos de conservación: Archivo de Trámite / 2 años – Archivo de Concentración / 8 años.

3.2 ÓRGANO INTERNO DE CONTROL

B.1.- Auditorías, revisiones y visitas a las áreas (Informes de resultados)

1.- Servidor público responsable del sistema o base de tratamiento.

Titular del Órgano Interno de Control.

2.- Funciones y obligaciones de las personas que tratan los datos personales.

Esta base de datos o sistema de tratamiento es con el fin de realizar las auditorías, revisiones y visitas a las diversas áreas de la Comisión e identificar plenamente a los servidores públicos que participan en dichos actos.

Asimismo, para publicar los informes de resultados de las auditorías al ejercicio presupuestal que se realicen y las aclaraciones que correspondan, en el portal de obligaciones de información de la CEAIP y en el Sistema de Portales de Obligaciones de Transparencia del Sistema Nacional de Transparencia (SIPOT), en cumplimiento a lo dispuesto en el artículo 95, fracción XXVIII de la Ley de Transparencia y Acceso a la Información Pública del Estado de Sinaloa.

El Órgano Interno de Control tiene facultades y funciones para realizar tratamiento de datos personales, esto con fundamento en los artículos 60 Bis C, fracciones II, III, IV, VII, VIII y X de la Ley de y 66 fracciones I, II, VIII y XVI del Reglamento Interior.

3.- Datos personales que se recaban y su finalidad.

DATO PERSONAL	FINALIDAD
Nombre	**Principal:** Los datos personales que sean proporcionados por los servidores públicos, serán protegidos y tratados con la
Identificación oficial (Domicilio, sexo, fecha de nacimiento, fotografía y nacionalidad)	

Clave Única de Registro de Población (CURP),	finalidad siguiente: realizar las auditorías, revisiones y visitas a las diversas áreas de la Comisión e identificar plenamente a los servidores públicos que participan en dichos actos.
Registro Federal de Contribuyentes (RFC)	
Estado Civil	
Datos laborales: Clave de número de empleado	
Datos académicos: Nivel de estudios y matrícula escolar	
Descuentos personales: Ahorro voluntario, hipoteca, seguro médico, seguro de auto.	

4.- Forma de obtención y medios de almacenamiento.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directa	**Físicos**

5.- Sitios de resguardo

[redacted]

6.- Servidores públicos que tienen acceso a los sistemas de datos personales.

Titular del Órgano Interno de Control, Jefe (a) del Departamento de Investigación, Analista adscrito (a) al área y la Coordinación de Archivos, una vez que se realiza la transferencia primaria al Archivo de Concentración para su resguardo.

7.- Encargado.

Proveedor/Tercero	No aplica.
Actividad	

Relación	
Instrumento jurídico que formaliza la prestación del servicio	

8.- Transferencias que se realizan.

No se realizan transferencias a terceros.

9.- Control archivístico.

Serie documental: CEAIP.14.00.02.00

Plazos de conservación: Ciclo de vida: Archivo de Trámite / 3 años – Archivo de Concentración / 3 años.

B.2.- Sistema de declaración de situación patrimonial, conflicto de intereses y constancia de presentación de declaración del ejercicio fiscal

1.- Servidor público responsable del sistema o base de tratamiento.

Titular de órgano interno de control.

2.- Funciones y obligaciones de las personas que tratan los datos personales.

Esta base de datos o sistema de tratamiento es con el fin de inscribir y mantener actualizada la información correspondiente a los Declarantes en el sistema de evolución patrimonial, de declaración de intereses y constancia de presentación de declaración fiscal; verificar la situación o posible actualización de algún Conflicto de Interés, según la información proporcionada; y llevar el seguimiento de la evolución y la verificación de la situación patrimonial de dichos Declarantes, en los términos de las leyes aplicables.

Asimismo, publicar la versión pública de las declaraciones patrimoniales en el Sistema de Portales de Obligaciones de Transparencia del Sistema Nacional de Transparencia (SIPOT), en cumplimiento a lo dispuesto en el artículo 95, fracción VIII de la Ley de Transparencia y Acceso a la Información Pública del Estado de Sinaloa.

El Órgano Interno de Control tiene facultades y obligaciones para realizar el tratamiento de datos personales, con fundamento en los artículos 28, 29, 30, 31, 32, 35, 36 y 46 de la Ley de Responsabilidades Administrativas del Estado de Sinaloa, 60 Bis E de la Ley de Transparencia y Acceso a la Información Pública del Estado de Sinaloa y 66, fracciones XIX, XX y XXI del Reglamento Interior.

3.- Datos personales que se recaban y su finalidad.

DATO PERSONAL	FINALIDAD
Nombre	**Principal:** Los datos personales que sean proporcionados por los servidores públicos, serán protegidos y tratados por el Órgano Interno de Control, con las finalidades siguientes: inscribir y mantener actualizada la información correspondiente a los Declarantes en el sistema de evolución patrimonial, de declaración de intereses y constancia de presentación de declaración fiscal; Verificar la situación o posible actualización de algún Conflicto de Interés, según la información proporcionada y; Llevar el seguimiento de la evolución y la verificación de la situación patrimonial de dichos Declarantes, en los términos de las leyes aplicables.
Clave Única de Registro de Población (CURP)	
Registro Federal de Contribuyentes y homoclave	
Correo electrónico institucional, personal y alterno	
Número telefónico personal y número celular personal	
Estado civil	
Régimen matrimonial	
País de nacionalidad	
Nacionalidad	
Domicilio	
Datos curriculares: Escolaridad, institución educativa, carrera o área de conocimiento, estatus, documento obtenido, fecha de obtención del documento, lugar donde se ubica la institución educativa	
Datos del empleo, cargo o comisión: Nivel/orden de gobierno, ámbito público, nombre del Ente Público, área de adscripción, empleo, cargo o comisión, tipo de	

contratación, nivel del empleo, cargo o comisión, función principal, fecha de toma de posesión/conclusión del empleo, teléfono de oficina y extensión y domicilio	
Experiencia Laboral: Ámbito/sector público, nivel/orden de gobierno, ámbito público, nombre, RFC, área de adscripción, empleo, cargo o comisión, sector al que pertenece, función principal, fecha de ingreso, fecha de egreso, lugar donde se ubica	
Datos de la Pareja y dependientes económicos: Nombre, fecha de nacimiento, R.F.C., relación/parentesco con el Declarante, Clave Única de Registro de Población, lugar donde reside, domicilio, actividad laboral, ámbito público, nombre del ente público, área de adscripción, empleo, cargo o comisión, función principal, salario mensual neto, fecha de ingreso al empleo	
Ingresos netos del Declarante, Pareja y/o dependientes económicos: Remuneración neta del Declarante por su cargo público, otros ingresos del Declarante, tipo de ingreso, ingreso neto del Declarante, ingreso neto de la pareja y/o dependientes económicos, total de ingresos netos percibidos por el Declarante, pareja y/o dependientes económicos	
Datos patrimoniales del declarante, pareja y/o dependientes económicos: Bienes inmuebles (tipo, titular, porcentaje de propiedad, superficie, nombre del tercero, RFC, forma de	

adquisición, forma de pago, transmisor, RFC, relación del transmisor, valor de adquisición, tipo de moneda, fecha de adquisición, datos del Registro Público de la Propiedad, ubicación), vehículos (tipo, titular, transmisor, nombre, RFC, relación del transmisor, marca, modelo, año, número de serie, tercero, nombre, RFC, forma de adquisición, forma de pago, valor, tipo de moneda, fecha de adquisición), bienes muebles (titular, tipo del bien, transmisor, nombre RFC, tercero, nombre, RFC, descripción general del bien, forma de adquisición, forma de pago, relación del transmisor con el titular, valor de adquisición, tipo de moneda y fecha de adquisición), inversiones, cuentas bancarias y otro tipo de valores activos (tipo de inversión, titular de la inversión, bancaria, tercero, fondos de inversión, organizaciones privadas y/o mercantiles, posesión de monedas o metales, seguros, valores bursátiles, afores y otros tipos, número de cuenta, contrato o póliza y saldo a la fecha), adeudos/pasivos (titular, tipo, número de cuenta o contrato, fecha de adquisición, monto original, tipo de moneda, tercero, nombre, RFC, otorgante del crédito, nombre o institución y RFC), préstamos y comodato por terceros (tipo y ubicación)	
<u>Declaración de intereses:</u> Participación en empresas (nombre de la empresa, RFC, porcentaje de participación de acuerdo a escrituras, tipo de participación,	

remuneración, lugar donde se ubica) participación en la toma de decisiones (tipo de institución, nombre, RFC, puesto, fecha de inicio, remuneración y lugar donde se ubica), apoyos o beneficios públicos (beneficiario, nombre del programa, institución otorgante, nivel u orden de gobierno, tipo de apoyo y forma de recepción del apoyo), representación (tipo, fecha de inicio, representante o representado, nombre o razón social, RFC, monto mensual, lugar donde se ubica y sector productivo al que pertenece), clientes principales (beneficio o ganancia directa, en su caso, actividades lucrativas, nombre o razón social, sector productivo al que pertenece, monto aproximado del beneficio o ganancia y lugar donde se ubica), beneficios privados (tipo, beneficiario, otorgante, nombre o razón sociales, forma de recepción del beneficio, monto mensual, tipo de moneda y sector productivo al que pertenece) y fideicomisos (tipo de fideicomiso, tipo de participación, RFC, nombre o razón social del fideicomitente y fiduciario, sector productivo al que pertenece y ubicación)	

4.- Forma de obtención y medios de almacenamiento.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directa	**Físicos y electrónicos**

5.- Sitios de resguardo

[redacted]

6.- Servidores públicos que tienen acceso a los sistemas de datos personales.

Titular del Órgano Interno de Control, Jefe del Departamento de Investigación, Analista adscrita al área, Coordinación de Sistemas Informáticos y la Coordinación de Archivos, una vez que se realiza la trasferencia primaria al Archivo de Concentración para su resguardo.

7.- Encargado.

Proveedor/Tercero	No aplica.
Actividad	
Relación	
Instrumento jurídico que formaliza la prestación del servicio	

8.- Transferencias que se realizan.

No se realizan transferencias a terceros.

9.Control archivístico.

Serie documental: CEAIP.14.00.04.00

Plazos de conservación: Archivo de Trámite / 3 años – Archivo de Concentración / 6 años.

3.3 UNIDAD DE TRANSPARENCIA

C.1.- Sistema de Expedientes de solicitudes de información pública.

1.- Servidor público responsable del sistema o base de tratamiento

Titular de la Unidad de Transparencia.

2.- Funciones y obligaciones de las personas que tratan los datos personales.

Esta base de datos o sistema de tratamiento es con el fin de dar trámite a las solicitudes que se presenten ante la CEAIP, notificar la respuesta a la solicitud, revisar el cumplimiento de los requisitos establecidos en la

Ley, contestar los medios de impugnación, en caso de que se presenten, dar cumplimiento a la publicación de las obligaciones de transparencia previstas en la Ley Local y General de Transparencia y Acceso a la información pública y para fines estadísticos sin vincular la información general con datos que hagan identificables a los solicitantes.

La Unidad de Transparencia tiene funciones para realizar tratamiento de datos personales, con fundamento en los artículos 68 fracción II, IV, V, VII, VIII y 127 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Sinaloa y 64 fracciones II, III, V, VI, VIII y XI, del Reglamento Interior.

3.- Datos personales que se recaban y su finalidad.

DATO PERSONAL	FINALIDAD
Nombre o, en su caso, los datos generales de su representante	**Principal:** Dar trámite a las solicitudes que se presenten, notificar la respuesta, revisar el cumplimiento de los requisitos establecidos en la Ley, contestar los medios de impugnación y dar cumplimiento a la publicación de las obligaciones de transparencia.
Domicilio	
Correo electrónico	

4.- Forma de obtención y medios de almacenamiento.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directa	**Físicos y electrónicos**

5.- Sitios de resguardo

[redacted]

6.- Servidores públicos que tienen acceso a los sistemas de datos personales.

Titular de la Unidad de Transparencia y Coordinación de Archivos, una vez que se realizan las transferencias al Archivo de Concentración para su resguardo.

7.-Encargado.

Proveedor/Tercero	No aplica.
Actividad	
Relación	
Instrumento jurídico que formaliza la prestación del servicio	

8.- Transferencias que se realizan.

No se realizan transferencias a terceros.

9.- Control archivístico.

Serie documental: CEAIP.13.00.03.00

Plazos de conservación: Archivo de Trámite / 2 años – Archivo de Concentración / 3 años.

C.2.- Sistema de solicitudes de ejercicio de derechos ARCO

1.- Servidor público responsable del sistema o base de tratamiento

Titular de la Unidad de Transparencia.

2.- Funciones y obligaciones de las personas que tratan los datos personales.

Esta base de datos o sistema de tratamiento es con el fin exclusivamente para dar atención a su solicitud de ejercicio de derechos ARCO que se presente ante CEAIP como responsable del tratamiento de los datos personales, así como con fines estadísticos.

La Unidad de Transparencia tiene funciones para realizar tratamiento de datos personales contenidos en esta base o sistema de tratamiento, con

fundamento en lo dispuesto en los artículos 63, 65, 72, 74, 112 y 114 de la Ley.

3.- Datos personales que se recaban y su finalidad.

DATO PERSONAL	FINALIDAD
Nombre o, en su caso, los datos generales de su representante	**Principal:** Para dar trámite al procedimiento de la solicitud de derechos ARCO, se solicita para poder demostrar la identidad del titular de dato o su representante.
Condición particular del titular (menor de edad, en estado de interdicción o incapacidad –sensible- o fallecido)	
Datos y documentos proporcionados en la descripción de la solicitud y para acreditar la identidad del titular y del representante, así como la personalidad	
Identificación oficial (Domicilio, sexo, fecha de nacimiento, fotografía, CURP)	

4.- Forma de obtención y medios de almacenamiento.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directa	**Físicos y electrónicos**

5.- Sitios de resguardo

[redacted]

6.- Servidores públicos que tienen acceso a los sistemas de datos personales.

Titular de la Unidad de Transparencia y Coordinación de Archivos, una vez que se realiza la transferencia primaria al Archivo de Concentración para su resguardo.

7.-Encargado.

Proveedor/Tercero	No aplica.
Actividad	
Relación	
Instrumento jurídico que formaliza la prestación del servicio	

8.- Transferencias que se realizan.

No se realizan transferencias a terceros.

9.- Control archivístico.

Serie documental: CEAIP.13.00.02.00

Plazos de conservación: Archivo de Trámite / 5 años – Archivo de Concentración / 5 años.

C.3.- Sistema de asesorías

1.- Servidor público responsable del sistema o base de tratamiento

Titular de la Unidad de Transparencia.

2.- Funciones y obligaciones de las personas que tratan los datos personales.

Esta base de datos o sistema de tratamiento es con el fin exclusivamente para llevar un registro de personas que atiende la unidad de transparencia, asimismo, los datos que se recaban son disociados para fines estadísticos.

La Unidad de Transparencia tiene funciones para realizar tratamiento de datos personales contenidos en esta base o sistema de tratamiento, con fundamento en los artículos 68 fracción III de la Ley de Transparencia; 114 fracción I de la Ley; y, 64 fracción IV, del Reglamento Interior.

3.- Datos personales que se recaban y su finalidad.

DATO PERSONAL	FINALIDAD
Nombre	**Principal:** Para dar trámite al procedimiento de la solicitud y asesorarlo en la presentación y seguimiento de las mismas.
Identificación oficial (Domicilio, sexo, fecha de nacimiento, fotografía, CURP)	
En algunos casos: Acta de nacimiento, acta de defunción, RFC y número de seguridad social.	

4.- Forma de obtención y medios de almacenamiento.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directa	**Físicos y electrónicos**

5.- Sitios de resguardo

[redacted]

6.- Servidores públicos que tienen acceso a los sistemas de datos personales.

Titular de la Unidad de Transparencia y Coordinación de Archivos, una vez que se realiza la transferencia primaria al Archivo de Concentración para su resguardo.

7.- Encargado.

Proveedor/Tercero	No aplica.
Actividad	
Relación	
Instrumento jurídico que formaliza la prestación del servicio	

8.- Transferencias que se realizan.

No se realizan transferencias a terceros.

9.-Control Archivístico.

Serie documental: CEAIP.13.00.04.00

Plazos de conservación: Archivo de Trámite / 2 años – Archivo de Concentración / 3 años.

C.4.- Sistema de informes sobre seguimiento de resolución en carácter de sujeto obligado.

1.- Servidor público responsable del sistema o base de tratamiento

Titular de la Unidad de Transparencia.

2.- Funciones y obligaciones de las personas que tratan los datos personales.

Esta base de datos o sistema es con el fin de dar tratamiento, seguimiento y cumplimiento a la denuncia presentada a la CEAIP.

La Unidad de Transparencia tiene funciones para realizar tratamiento de datos personales contenidos en esta base o sistema de tratamiento, con lo dispuesto en los artículos 68, fracción I en relación con el 114 de la Ley de Transparencia y 64 fracción XVI del Reglamento Interior.

3.- Datos personales que se recaban y su finalidad.

DATO PERSONAL	FINALIDAD
Nombre	**Principal:** Para dar tratamiento, seguimiento y cumplimiento a la denuncia y recursos de revisión en contra de la Comisión.
Correo electrónico	

4.- Forma de obtención y medios de almacenamiento.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directa	**Físicos y electrónicos**

5.- Sitios de resguardo.

[redacted]

6.- Servidores públicos que tienen acceso a los sistemas de datos personales.

Titular de la Unidad de Transparencia y Coordinación de Archivos, una vez que se realiza la transferencia primaria al Archivo de Concentración para su resguardo.

7.- Encargado.

Proveedor/Tercero	No aplica.
Actividad	
Relación	
Instrumento jurídico que formaliza la prestación del servicio	

8.- Transferencias que se realizan.

No se realizan transferencias a terceros.

9. Control archivístico.

Serie documental: CEAIP.13.00.06.00

Plazos de conservación: Archivo de Trámite / 2 años – Archivo de Concentración / 3 años.

3.4 DIRECCIÓN JURÍDICA CONSULTIVA

D.1.- Procedimientos de Denuncias de Obligaciones de Transparencia

1.- Servidor público responsable del sistema o base de tratamiento

Titular de la Dirección Jurídica Consultiva

2.-Funciones y obligaciones de las personas que tratan datos personales:

Esta base de datos o sistema es con el fin exclusivo de recibir, registrar y tramitar las denuncias que sean presentadas.

La Dirección Jurídica Consultiva tiene funciones para realizar el tratamiento de datos personales contenidos en esta base o sistema de, con fundamento en lo dispuesto en los artículos 113 y 114, fracciones III, IV y V y del 95 al 106 de la Ley de Transparencia.

3.- Datos personales que se recaban y su finalidad.

DATO PERSONAL	FINALIDAD
Nombre del denunciante	**Principal:** Para dar trámite al procedimiento de la denuncia.
Domicilio	
Correo electrónico	
Fecha de nacimiento	
Nivel educativo	

4.- Forma de obtención y medios de almacenamiento.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directa	**Físicos y electrónicos**

5.- Sitios de resguardo

[redacted]

6.- Servidores públicos que tienen acceso a los sistemas de datos personales.

Director Jurídico Consultivo, Analistas Jurídicos adscritos al área, Analistas Notificadores y Coordinación de Archivos, una vez que se realiza la transferencia primaria al Archivo de Concentración para su resguardo.

7.- Encargado.

Proveedor/Tercero	No aplica.
Actividad	
Relación	
Instrumento jurídico que formaliza la prestación del servicio	

8.- Transferencias que se realizan.

No se realizan transferencias a terceros.

9.Control archivístico.

Serie documental: CEAIP.04.00.01.00 DOT

Plazos de conservación: Archivo de Trámite / 5 años – Archivo de Concentración / 10 años.

D.2.- Procedimientos de Verificación de Datos Personales (denuncias).

1.- Servidor público responsable del sistema o base de tratamiento.

Titular de la Dirección Jurídica Consultiva.

2.- Funciones y obligaciones de las personas que tratan los datos personales.

Esta base de datos o sistema es con el fin exclusivo para recibir, registrar y tramitar las denuncias.

La Dirección Jurídica Consultiva tiene funciones para realizar tratamiento de datos personales contenidos en esta base o sistema de tratamiento, de conformidad con lo dispuesto en los artículos 157 al 180 de la Ley; 33 fracción XX y 46 fracción I del Reglamento Interior.

3.- Datos personales que se recaban y su finalidad.

DATO PERSONAL	FINALIDAD
Nombre del denunciante, o en su caso, de su representante	**Principal:** Para dar trámite al procedimiento de la denuncia y realizar las notificaciones correspondientes.
Domicilio o medio para recibir notificaciones	
La relación de hechos y elementos probatorios	
Nombre del responsable denunciado y su domicilio, o en su caso, los datos para su identificación y/o ubicación	
Firma del denunciante, o en su caso, de su representante, en caso de no saber firmar, bastará la huella digital	
Datos de identificación	

4.- Forma de obtención y medios de almacenamiento.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directa	**Físicos**

5.- Sitios de resguardo.

[redacted]

6.- Servidores públicos que tienen acceso a los sistemas de datos personales.

Director Jurídico Consultivo, Analistas Jurídicos adscritos al área, Analistas Notificadores, Dirección de Datos Personales y Coordinación de Archivos, una vez que se realiza la transferencia primaria al Archivo de Concentración para su resguardo.

7.- Encargado.

Proveedor/Tercero	No aplica.
Actividad	
Relación	
Instrumento jurídico que formaliza la prestación del servicio	

8.- Transferencias que se realizan.

No se realizan transferencias a terceros.

9.Control archivístico.

Serie documental: No cuenta con serie documental.

Plazos de conservación: No cuenta.

D.3.- Procedimientos Administrativos Sancionatorios.

1.- Servidor público responsable del sistema o base de tratamiento.

Titular de la Dirección Jurídica Consultiva.

2.- Funciones y obligaciones de las personas que tratan los datos personales.

Esta base de datos o sistema es con el fin exclusivo de dar trámite a las causas de sanción por incumplimiento de las obligaciones de transparencia.

La Dirección Jurídica Consultiva tiene funciones para realizar el tratamiento de datos personales contenidos en esta base o sistema de

tratamiento, con lo dispuesto en los artículos 201, 203 y 205 de la Ley de Transparencia; 46 fracción IV y 105 del Reglamento Interior.

3.- Datos personales que se recaban y su finalidad.

DATO PERSONAL	FINALIDAD
Nombre del servidor público	**Principal:** Para dar trámite al procedimiento administrativo sancionador y realizar las notificaciones correspondientes.
Cargo o nombramiento	
Representante legal	
Domicilio particular	
Correo electrónico	
Teléfono	

4.- Forma de obtención y medios de almacenamiento.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directa	**Físicos**

5.- Sitios de resguardo.

[redacted]

6.- Servidores públicos que tienen acceso a los sistemas de datos personales.

Director Jurídico Consultivo, Analistas Jurídicos, Analistas Notificador adscritos al área y Coordinación de Archivos, una vez que se realiza la transferencia primaria al Archivo de Concentración para su resguardo.

7.- Encargado.

Proveedor/Tercero	No aplica

Actividad	
Relación	
Instrumento jurídico que formaliza la prestación del servicio	

8.- Transferencias que se realizan.

No se realizan transferencias a terceros.

9.- Control archivístico.

Serie documental: CEAIP.04.00.02.00

Plazos de conservación: Archivo de Trámite / 5 años – Archivo de Concentración / 10 años.

3.5 SECRETARÍA EJECUTIVA

E.1.- Sistema de Ejecución de Cumplimientos e Incumplimientos.

1.- Servidor público responsable del sistema o base de tratamiento.

Titular de la Secretaría ejecutiva.

2.- Funciones y obligaciones de las personas que tratan los datos personales.

Esta base de datos o sistema es con el fin exclusivo de informar a los recurrentes y sujetos obligados el cumplimiento o incumplimiento de la resolución emitida en el recurso de revisión.

La Secretaría Ejecutiva tiene funciones para realizar tratamiento de datos personales contenidos en esta base o sistema de tratamiento, con lo dispuesto en los artículos 189, 190 de la Ley de Transparencia; y 42 fracción XIII del Reglamento Interior.

3.- Datos personales que se encuentran en la base de datos y su finalidad.

DATO PERSONAL	FINALIDAD
Nombre	**Principal:** Para dar trámite al cumplimiento o incumplimiento de resoluciones de recursos de revisión, así como para realizar las notificaciones correspondientes.
Correo electrónico	
Domicilio	

4.- Forma de obtención y medios de almacenamiento.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directa	**Físicos**

5.- Sitios de resguardo.

[redacted]

6.- Servidores públicos que tienen acceso a los sistemas de datos personales.

Secretaria Ejecutiva, Analistas adscritos a la Secretaría Ejecutiva, Ponencias y Coordinación de Archivos, una vez que se realiza la transferencia primaria al Archivo de Concentración para su resguardo.

7.- Encargado.

Proveedor/Tercero	No aplica.
Actividad	
Relación	
Instrumento jurídico que formaliza la prestación del servicio	

8.- Transferencias que se realizan.

No se realizan transferencias a terceros.

9.Control Archivístico.

Serie documental: CEAIP.03.00.03.00

Plazos de conservación: Archivo de Trámite / 1 año – Archivo de Concentración / 5 años.

3.6 UNIDAD DE GOBIERNO ABIERTO

F.1.- Sistema de Registro de participantes de Gobierno Abierto

1.- Servidor público responsable del sistema o base de tratamiento

Titular de la Unidad de Gobierno Abierto.

2.- Funciones y obligaciones de las personas que tratan los datos personales.

Esta base de datos o sistema de tratamiento es con el fin de integrar un registro de participantes o interesados en participar en el ejercicio de Gobierno Abierto.

La Comisión y la Unidad de Gobierno Abierto tiene facultades y obligaciones para realizar tratamiento de datos personales contenidos en esta base o sistema de tratamiento, de conformidad con lo dispuesto en el artículo 32 fracción XXVII y 85 de la Ley de Transparencia; 62 fracción I, III y IV del Reglamento Interior.

3.- Datos personales que se recaban y su finalidad.

DATO PERSONAL	FINALIDAD
Nombre	**Principal:** Para dar seguimiento a la integración del registro de participantes o interesados en el ejercicio de Gobierno Abierto.
Apellido	
Correo electrónico	

4.- Forma de obtención y medios de almacenamiento.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directa del titular (participante o interesado)	**Electrónicos**

5.- Sitios de resguardo.

[redacted]

6.- Servidores públicos que tienen acceso a los sistemas de datos personales.

Titular de la Unidad de Gobierno Abierto, personal de la Dirección de Capacitación y Vinculación Ciudadana.

7.- Encargado.

Proveedor/Tercero	No aplica
Actividad	
Relación	
Instrumento jurídico que formaliza la prestación del servicio	

8.- Transferencias que se realizan.

No se realizan transferencias a terceros.

9. Control archivístico.

Serie documental: No cuenta con serie documental

Plazos de conservación: 3 años

F.2.- Sistema de listas de asistencia de eventos de Gobierno Abierto

1.- Servidor público responsable del sistema o base de tratamiento

Titular de la Unidad de Gobierno Abierto.

2.-Funciones y obligaciones de las personas que tratan los datos personales:

Esta base de datos o sistema de tratamiento es con el fin de integrar un registro de asistentes a los diferentes eventos realizados por la Unidad de Gobierno Abierto.

La Comisión y la Unidad de Gobierno Abierto tienen atribuciones y funciones para realizar tratamiento de datos personales contenidos en esta base o sistema de tratamiento, de conformidad con lo dispuesto en el artículo 32 fracción XXVII y 85 de la Ley de Transparencia; 62 fracciones I, III y IV del Reglamento Interior.

3.- Datos personales que se recaban y su finalidad.

DATO PERSONAL	FINALIDAD
Nombre	**Principal:** Integrar un registro de asistentes a los diferentes eventos realizados por la Unidad de Gobierno Abierto.
Cargo o Puesto	
Correo electrónico	
Organización a la que pertenece	
Teléfono	

4.- Forma de obtención y medios de almacenamiento.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directa	**Electrónicos y Físicos**

5.- Sitios de resguardo

[redacted]

6.- Servidores públicos que tienen acceso a los sistemas de datos personales.

Titular de la Unidad de Gobierno Abierto

7.- Encargado.

Proveedor/Tercero	No aplica
Actividad	
Relación	
Instrumento jurídico que formaliza la prestación del servicio	

8.- Transferencias que se realizan.

No se realizan transferencias a terceros.

9.Control archivístico.

No cuenta con serie documental

Plazo de conservación: 3 años

3.7 DIRECIÓN DE CAPACITACIÓN Y VINCULACIÓN CIUDADANA

G.1.- Sistema de Registro de Capacitación para Sujetos Obligados

1.- Servidor público responsable del sistema o base de tratamiento.

Titular de la Dirección de Capacitación y Vinculación Ciudadana y jefe (a) del Departamento de Vinculación.

2.- Funciones y obligaciones de las personas que tratan los datos personales.

Esta base de datos o sistema de tratamiento es con el objeto de llevar a cabo un registro de los asistentes a las capacitaciones realizadas por la Comisión en materia de transparencia, acceso a la información pública y

protección de datos personales, difundir la capacitación a través de la página oficial y redes sociales, generar constancias y estadísticas que evidencien el trabajo realizado, así como integrar el acervo de imágenes y fotografías que respalden las actividades y eventos.

La Comisión y la Dirección de Capacitación y Vinculación Ciudadana tienen atribuciones y funciones para realizar el tratamiento de datos personales contenidos en esta base o sistema de tratamiento, con fundamento en los artículos 32, fracción XI de la Ley de Transparencia; 118 fracción XVI y XXII de la Ley; 50 fracciones II, IV Y VIII del Reglamento Interior.

3.- Datos personales que se recaban y su finalidad.

DATO PERSONAL	FINALIDAD
Nombre	**Principal:** Llevar a cabo un registro de los asistentes a las capacitaciones.
Correo electrónico	Mantener contacto con los sujetos obligados, a través del cual se envíe de ser el caso las ligas de acceso a zoom, envío de oficios, invitaciones y material correspondiente a la capacitación impartida.
Sexo	Generar las estadísticas con perspectiva de género.
Firma	Formalizar el requerimiento de la capacitación solicitada mediante oficio cuando es de manera presencial.

4.- Forma de obtención y medios de almacenamiento.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directa	**Físicos y Electrónicos**

5.- Sitios de resguardo

[redacted]

6.- Servidores públicos que tienen acceso a los sistemas de datos personales.

7.- Encargado.

Proveedor/Tercero	No aplica
Actividad	
Relación	
Instrumento jurídico que formaliza la prestación del servicio	

8.- Transferencias que se realizan.

No se realizan transferencias a terceros.

9. Control archivístico.

Serie documental: CEAIP.06.00.02.00

Plazos de conservación: Archivo de Trámite / 2 años – Archivo de Concentración / 5 años.

G.2.- Sistema de Registro de Socialización.

1.- Servidor público responsable del sistema o base de tratamiento.

Titular de la Dirección de Capacitación y Vinculación Ciudadana y jefe (a) del Departamento de Vinculación.

2.- Funciones y obligaciones de las personas que tratan los datos personales.

Esta base de datos o sistema de tratamiento es con el fin de llevar a cabo un registro de los asistentes a las socializaciones realizadas por la CEAIP, en materia de transparencia, acceso a la información pública y protección de datos personales impartidas por personal de la Comisión; así como difundir el resultado de ellas en la página oficial y las redes sociales, generar las constancias respectivas y las estadísticas del trabajo realizado en cumplimiento de las atribuciones e integrar el acervo de imágenes y fotografías que respalden las actividades y eventos realizados.

La Comisión y la Dirección de Capacitación y Vinculación Ciudadana tiene atribuciones y funciones para realizar tratamiento de datos personales contenidos en esta base o sistema de tratamiento, con fundamento en los artículos 32, fracción IX de la Ley de Transparencia; 118 fracciones VIII y XXI de la Ley; y 50 fracciones III, IV, VI y VIII del Reglamento Interior.

3.- Datos personales que se recaban y su finalidad.

DATO PERSONAL	FINALIDAD
Nombre	**Principal:** Llevar a cabo un registro de los asistentes a las socializaciones.
Correo electrónico	Mantener contacto con los ciudadanos, a través del cual se envíe de ser el caso las ligas de acceso a zoom, envío de oficios, invitaciones y material correspondiente a la socialización impartida.
Sexo	Registrar a los asistentes a las socializaciones y elaborar las estadísticas con perspectiva de género.
Ocupación	
Escolaridad	
Firma	Formalizar el requerimiento de la socialización solicitada mediante oficio cuando es de manera presencial.

4.- Forma de obtención y medios de almacenamiento.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directa	**Físicos y Electrónicos**

5.- Sitios de resguardo.

[redacted]

6.- Servidores públicos que tienen acceso a los sistemas de datos personales.

Personal de la Dirección de Capacitación y Vinculación Ciudadana, Titular de la Coordinación de Sistemas Informáticos y Coordinación de Archivos, una vez que se realiza la transferencia primaria al Archivo de Concentración para su resguardo.

7.- Encargado.

Proveedor/Tercero	No aplica
Actividad	
Relación	
Instrumento jurídico que formaliza la prestación del servicio	

8.- Transferencias que se realizan.

No se realizan transferencias a terceros.

9. Control archivístico.

Serie documental: CEAIP.06.00.03.00

Plazos de conservación: Archivo de Trámite / 2 años – Archivo de Concentración / 5 años.

G.3.- Sistema de Registro de Concursos.

1.- Servidor público responsable del sistema o base de tratamiento.

Titular de la Dirección de Capacitación y Vinculación Ciudadana y jefe (a) del Departamento de Vinculación.

2.- Funciones y obligaciones de las personas que tratan datos personales.

Esta base de datos o sistema de tratamiento es con el fin de llevar a cabo un registro de los participantes de los concursos realizados por la Comisión, a fin de poder contactar y premiar a los que resulten ganadores, difundir los concursos a través de la página oficial y las redes sociales de la misma, generar las constancias y estadísticas que evidencien el trabajo realizado por la Comisión o que ayuden al cumplimiento de sus atribuciones, integrar el acervo de imágenes y fotografías que respalden las actividades y eventos realizados, cumplir con lo establecido en la convocatoria y bases del concurso, publicar el nombre de los ganadores del concurso y otorgar los premios previstos.

La Comisión y la Dirección de Capacitación y Vinculación Ciudadana tiene atribuciones y funciones para realizar tratamiento de datos personales contenidos en esta base o sistema de tratamiento, con fundamento en los artículos 32, fracción IX de la Ley de Transparencia; 118 fracción XXI de la Ley; y 50 fracción VII del Reglamento Interior.

3.- Datos personales que se recaban y su finalidad.

DATO PERSONAL	FINALIDAD
Nombre	**Principal:** Llevar a cabo un registro de los participantes de los concursos realizados.
Sexo	**Principal:** Registrar y elaborar las estadísticas de los participantes a los concursos realizados.
Edad	**Principal:** Para corroborar los requisitos para participar en el concurso.
Lugar de residencia	

Domicilio	**Principal:** A fin de conocer de dónde es el participante y corroborar requisitos previstos en la convocatoria.
Correo electrónico	**Principal:** Mantener el contacto con el participante y poder dar seguimiento al concurso en caso de que resultara ganador.
Número de teléfono fijo o celular	**Principal:** Mantener el contacto con el participante y poder dar seguimiento al concurso en caso de que resultara ganador.
En caso de menores de edad los datos contenidos en el acta de nacimiento del menor y en la identificación oficial del padre o tutor.	**Principal:** Registrar a los participantes previa autorización del padre, madre o tutor.

4.- Forma de obtención y medios de almacenamiento.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directa	**Físicos y Electrónicos**

5.- Sitios de resguardo.

[redacted]

6.- Servidores públicos que tienen acceso a los sistemas de datos personales.

Personal de la Dirección de Capacitación y Vinculación Ciudadana, Titular de la Coordinación de Sistemas Informáticos y Coordinación de Archivos, una vez que se realiza la transferencia primaria al Archivo de Concentración para su resguardo.

7.- Encargado.

Proveedor/Tercero	No aplica
Actividad	
Relación	
Instrumento jurídico que formaliza la prestación del servicio	

8.- Transferencias que se realizan.

No se realizan transferencias a terceros.

9.- Control archivístico.

Serie documental: CEAIP.06.00.05.00

Plazos de conservación: Archivo de Trámite / 2 años – Archivo de Concentración / 5 años.

G.4 Directorio de Unidades De Transparencia.

1.- Servidor público responsable del sistema o base de tratamiento.

Titular de la Dirección de Capacitación y Vinculación Ciudadana y jefe (a) del Departamento de Vinculación.

2.- Funciones y obligaciones de las personas que tratan datos personales.

Esta base de datos o sistema de tratamiento es con el fin de llevar a cabo un registro de cada uno de los titulares de las Unidades de Transparencia (UT) de los sujetos obligados y difundirlos en el portal institucional de la Comisión con el objetivo de facilitar a los particulares el establecimiento de contacto y comunicación la respectiva UT, para que si así lo requieren, éstas los auxilien en la elaboración de solicitudes de acceso a la información y en su caso orientarlos sobre los sujetos obligados competentes conforme a la normatividad aplicable.

La Comisión tiene atribuciones para realizar tratamiento de datos personales contenidos en esta base o sistema de tratamiento, con fundamento en los artículos 32, fracción IX de la Ley de Transparencia.

3.- Datos personales que se recaban y su finalidad.

DATO PERSONAL	FINALIDAD
Nombre	**Principal:** Llevar a cabo un registro de los servidores públicos, titulares de la UT.
Correo electrónico personal (En algunos casos, los sujetos obligados no cuentan con correos institucionales y por ende los TUT autorizan y consienten el uso de correos electrónicos personales como medio de comunicación).	**Principal:** Establecimiento de contacto y comunicación.

4.- Forma de obtención y medios de almacenamiento.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directa	**Electrónicos**

5.- Sitios de resguardo.

[redacted]

6.- Servidores públicos que tienen acceso a los sistemas de datos personales.

Personal de la Dirección de Capacitación y Vinculación Ciudadana.

7.- Encargado.

Proveedor/Tercero	No aplica
Actividad	
Relación	
Instrumento jurídico que formaliza la prestación del servicio	

8.- Transferencias que se realizan.

No se realizan transferencias a terceros.

9.- Control archivístico.

Serie documental: No cuenta con serie documental.

Plazos de conservación: No cuenta con plazos de conservación.

3.8 DEPARTAMENTO DE COMUNICACIÓN

H.1- Sistema de evidencias y publicidad.

1.- Servidor público responsable del área administrativa

Titular de la jefatura del departamento de comunicación.

2.- Funciones y obligaciones de las personas que tratan los datos personales.

Esta base de datos o sistema de tratamiento es el informar y difundir, a través de diversos medios digitales a la sociedad acerca de las actividades de la Comisión, vinculadas a temas de transparencia, rendición de cuentas, acceso a la información pública y protección de datos personales, asimismo realizar labores de difusión con los sujetos obligados y otras instituciones del sector público o privado, para el desarrollo de actividades por la cultura de la transparencia.

El Departamento de Comunicación y Diseño de la CEAIP tiene funciones para realizar tratamiento de datos personales contenidos en esta base o sistema de tratamiento, con lo dispuesto en los artículos 32 fracción IX de la Ley y 118 fracción VIII de la LPDPPSOES.

3.- Datos personales que se recaban y su finalidad.

DATO PERSONAL	FINALIDAD
Imagen	**Principal:** Registrar en fotografías y video los eventos, capacitaciones, o cualquier otra actividad, así como asistentes para demostrar con evidencias la realización de las acciones y

	asistencia de personas a los mismos.

4.- Forma de obtención y medios de almacenamiento.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directa	**Electrónicos**

5.- Sitios de resguardo.

[redacted]

6.- Servidores públicos que tienen acceso a los sistemas de datos personales.

7.- Terceros encargados de datos personales.

Proveedor/Tercero	No aplica
Actividad	
Relación	
Instrumento jurídico que formaliza la prestación del servicio	

8.- Transferencias que se realizan.

No se realizan transferencias a terceros.

9.- Control archivístico.

Serie documental: No cuenta con serie documental.

Plazos de conservación: No cuenta con plazos de conservación establecidos.

H.2- Sistema de credencialización oficial de la CEAIP.

1.- Servidor público responsable del área administrativa.

Analista de diseño.

2.- Funciones y obligaciones de las personas que tratan datos personales.

Esta base de datos o sistema de tratamiento es con el fin exclusivo de generar las identificaciones oficiales de los servidores públicos de la CEAIP.

El Comisionado Presidente por medio de Diseño tienen funciones para realizar tratamiento de datos personales contenidos en esta base o sistema de tratamiento, de conformidad con lo dispuesto en los artículos 168 fracción I de la Ley; y 33 fracción XXVII del Reglamento Interior.

3.- Datos personales que se recaban y su finalidad.

DATO PERSONAL	FINALIDAD
Nombre y firma de los servidores públicos.	**Principal:** Generar las identificaciones oficiales de los servidores públicos de la CEAIP.
Fotografía del acreditado.	

4.- Forma de obtención y medios de almacenamiento.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directa: Del Titular	**Electrónicos**

5.- Sitios de resguardo.

[redacted]

6.- Servidores públicos que tienen acceso a los sistemas de datos personales.

Analista de Diseño.

7.- Encargado.

Proveedor/Tercero	No aplica
Actividad	
Relación	
Instrumento jurídico que formaliza la prestación del servicio	

8.- Transferencias que se realizan.

No se realizan transferencias a terceros.

9. Control archivístico.

Serie documental: No cuenta con serie documental.

Plazos de conservación: No tiene establecidos.

3.9 COORDINACIÓN DE SISTEMAS INFORMÁTICOS

I.1.- Sistema de Reuniones por la Plataforma ZOOM

1.- Servidor público responsable del sistema o base de tratamiento.

Titular de la Coordinación de Sistemas Informáticos.

2.- Funciones y obligaciones de las personas que tratan datos personales.

Esta base de datos o sistema de tratamiento es con el fin exclusivo de generar las reuniones virtuales a través de la Plataforma ZOOM.

La Coordinación de Sistemas Informáticos tiene facultades para realizar tratamiento de datos personales contenidos en esta base o sistema de tratamiento, con lo dispuesto en el artículo 60 fracción VII del Reglamento Interior.

3.- Datos personales que se recaban y su finalidad.

DATO PERSONAL	FINALIDAD
Nombres de asistentes	**Principal:** Identificación de asistentes a la reunión.
Imagen	

4.- Forma de obtención y medios de almacenamiento.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directa	**Electrónicos**

5.- Sitios de resguardo.

[redacted]

6.- Servidores públicos que tienen acceso a los sistemas de datos personales.

Personal de la Coordinación de Sistemas Informáticos y la Dirección de Capacitación y Vinculación Ciudadana, previa solicitud para corroborar la asistencia de los participantes.

7.- Encargado.

Proveedor/Tercero	No aplica
Actividad	
Relación	
Instrumento jurídico que formaliza la prestación del servicio	

8.- Transferencias que se realizan.

No se realizan transferencias a terceros.

9. Control archivístico.

Serie documental: No cuenta con serie documental.

Plazos de conservación: No se encuentra establecido.

I.2.- Sistema de Correo Electrónico Institucional.

1.- Servidor público responsable del sistema o base de tratamiento.

Titular de la Coordinación de Sistemas Informáticos.

2.- Funciones y obligaciones de las personas que tratan datos personales.

Esta base de datos o sistema de tratamiento es con el fin exclusivo de crear las cuentas y administrar los correos electrónicos institucionales, así como resguardar los correos electrónicos particulares que en su caso ingresen a este sistema.

La Coordinación de Sistemas Informáticos tiene facultades para realizar el tratamiento de datos personales contenidos en esta base o sistema de tratamiento, con fundamento en el artículo 60 fracción VIII del Reglamento Interior.

3.- Datos personales que se recaban y su finalidad.

DATO PERSONAL	FINALIDAD
Nombre del servidor público	**Principal:** Crear las cuentas y administrar los correos electrónicos que pueden ser particulares y servidores públicos desde los cuales se envía información al personal de la CEAIP.

Nombre de particulares y correos electrónicos no oficiales	**Principal:** Administrar y resguardar los mensajes recibidos en el sistema.

4.- Forma de obtención y medios de almacenamiento.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directa	**Electrónicos**

5.- Sitios de resguardo.

[redacted]

6.- Servidores públicos que tienen acceso a los sistemas de datos personales.

Coordinador de Sistemas Informáticos.

7.- Encargado.

Proveedor/Tercero	Empresa
Actividad	Alojamiento web (nube)
Relación	Proveedor de servicio de hosting
Instrumento jurídico que formaliza la prestación del servicio	Contrato que establece términos y condiciones del servicio

8.- Transferencias que se realizan.

No se realizan transferencias a terceros.

9. Control archivístico.

Serie documental: No cuenta con serie documental

Plazos de conservación: Las definidas en cada contrato.

I.3.- Sistema de Tickets para Soporte

1.- Servidor público responsable del sistema o base de tratamiento.

Titular de la Coordinación de Sistemas Informáticos.

2.-Funciones y obligaciones de las personas que tratan datos personales.

Esta base de datos o sistema de tratamiento es con el fin exclusivo de brindar atención, asistencia y apoyo técnico a los servidores públicos de los sujetos obligados y de la CEAIP.

La Comisión y la Coordinación de Sistemas Informáticos tienen atribuciones y facultades para realizar tratamiento de datos personales contenidos en esta base o sistema de tratamiento, con fundamento en el artículo 32 fracción XI de la Ley de Transparencia; y 60, fracciones VII y VIII del Reglamento Interior.

3.- Datos personales que se recaban y su finalidad.

DATO PERSONAL	FINALIDAD
Correo electrónico particular	**Principal:** Atención a los Sujetos Obligados y asistencia técnica a los servidores públicos de la CEAIP.
Correo electrónico	

4.- Forma de obtención y medios de almacenamiento.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directa	**Electrónicos**

5.- Sitios de resguardo.

[redacted]

6.- Servidores públicos que tienen acceso a los sistemas de datos personales.

Coordinador de Sistemas Informáticos, Analista de sistemas y Coordinador Estatal de la PNT.

7.- Encargado.

Proveedor/Tercero	Empresa
Actividad	Alojamiento web (nube)
Relación	Proveedor de servicio de hosting
Instrumento jurídico que formaliza la prestación del servicio	Contrato que establece términos y condiciones del servicio.

8.- Transferencias que se realizan.

No se realizan transferencias a terceros.

9. Control archivístico.

Serie documental: No cuenta con serie documental

Plazos de conservación: Las definidas en cada contrato.

I.4.- Sistema de Videovigilancia.

1.- Servidor público responsable del sistema o base de tratamiento.

Titular de la Coordinación de Sistemas Informáticos.

2.- Funciones y obligaciones de las personas que tratan datos personales.

Esta base de datos o sistema de tratamiento tiene por objeto recabar la imagen de las personas que ingresan y transitan en las oficinas de la Comisión y serán utilizadas para vigilar la seguridad e integridad de los servidores públicos, visitantes y de las instalaciones.

La Coordinación de Sistemas Informáticos tiene facultades para realizar tratamiento de datos personales contenidos en esta base o sistema de tratamiento, con fundamento en el numeral décimo primero de los Lineamientos Internos para el uso de videovigilancia en las instalaciones de la Comisión.

3.- Datos personales que se recaban y su finalidad.

DATO PERSONAL	FINALIDAD
Imagen	**Principal:** Recabar la imagen de las personas que ingresan y transitan en las oficinas y serán utilizadas para vigilar la seguridad e integridad de los servidores públicos y visitantes, así como de las instalaciones de la Comisión e identificar, en su caso, conductas de riesgo o constitutivas de delito.

4.- Forma de obtención y medios de almacenamiento.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directa	**Electrónicos**

5.- Sitios de resguardo

[redacted]

6.- Servidores públicos que tienen acceso a los sistemas de datos personales.

Titular de la Coordinación de Sistemas Informáticos, el Pleno y personal autorizado por éste.

7.- Encargado.

Proveedor/Tercero	No aplica
Actividad	
Relación	
Instrumento jurídico que formaliza la prestación del servicio	

8.- Transferencias que se realizan.

No se realizan transferencias a terceros.

9.-Control archivístico.

Serie documental: No cuenta con serie documental.

Plazos de conservación: 60 días naturales.

I.5.- Sistema de Registro de Asistencia del Personal de la Ceaip.

1.- Servidor público responsable del sistema o base de tratamiento.

Titular de la Coordinación de Sistemas Informáticos.

2.- Funciones y obligaciones de las personas que tratan datos personales.

Esta base de datos o sistema de tratamiento es con el fin de controlar y registrar la asistencia de los servidores públicos de la CEAIP que ocupen plaza de confianza y honorarios.

La Coordinación de Sistemas Informáticos tiene facultades y obligaciones para realizar tratamiento de datos personales contenidos en esta base o sistema de tratamiento, con fundamento en lo dispuesto en los artículos 28, fracción XXXVIII, 60, fracciones II, VII y XI del Reglamento Interior de la Comisión Estatal para el Acceso a la Información Pública de Sinaloa.

3.- Datos personales que se recaban y su finalidad.

DATO PERSONAL	FINALIDAD
Nombre	

Huella digital	**Principal:** Controlar y registrar la asistencia de los servidores públicos de la CEAIP que ocupen plaza de confianza y honorarios.

4.- Forma de obtención y medios de almacenamiento.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directa	**Electrónicos**

5.- Sitios de resguardo.

[redacted]

6.- Servidores públicos que tienen acceso a los sistemas de datos personales.

Titular de la Coordinación de Sistemas Informáticos y el titular de la Dirección de Administración, quien únicamente tiene acceso al registro de asistencia del personal, pero no tiene acceso a la huella digital.

7.- Encargado.

Proveedor/Tercero	No aplica
Actividad	
Relación	
Instrumento jurídico que formaliza la prestación del servicio	

8.- Transferencias que se realizan.

No se realizan transferencias a terceros.

9.Control archivístico.

Serie documental: No cuenta con serie documental.

Plazos de conservación: No cuenta con plazos de conservación.

I.6.- Sistema de firma digital de Comisionados.

1.- Servidor público responsable del sistema o base de tratamiento

Titular de la Coordinación de Sistemas Informáticos.

2.- Funciones y obligaciones de las personas que tratan datos personales.

Esta base de datos o sistema de tratamiento es con el fin de utilizar las firmas digitales de los Comisionados para plasmarlas en las constancias o reconocimientos expedidos por la CEAIP.

3.- Datos personales que se recaban y su finalidad.

DATO PERSONAL	FINALIDAD
Firma oficial	**Principal:** Utilizar las firmas digitales de los Comisionados para plasmarlas en las constancias o reconocimientos expedidos por la CEAIP.

4.- Forma de obtención y medios de almacenamiento físico o electrónico.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directa	**Electrónicos**

5.- Sitios de resguardo.

[redacted]

6.- Servidores públicos que tienen acceso a los sistemas de datos personales.

Analista de sistemas.

7.- Encargado.

Proveedor/Tercero	No aplica
Actividad	
Relación	
Instrumento jurídico que formaliza la prestación del servicio	

8.- Transferencias que se realizan.

No se realizan transferencias a terceros.

9. Organización y Ciclo de vida.

Serie documental: No cuenta con serie documental.

Plazos de conservación: No cuenta con plazos establecidos.

I.7- Sistema de Directorio de la CEAIP

1.- Servidor público responsable del área administrativa.

Titular de la Coordinación de los Sistemas Informáticos.

2.- Funciones y obligaciones de las personas que tratan los datos personales.

Esta base de datos o sistema de tratamiento es con el fin de publicar el Directorio de los servidores públicos de la CEAIP y difundirlo a través de la página oficial.

3.- Datos personales que se recaban y su finalidad.

DATO PERSONAL	FINALIDAD
Imagen	**Principal:** Publicar el Directorio de los servidores públicos de la CEAIP
Fotografía	

	y difundirlo a través de la página oficial.

4.- Forma de obtención y medios de almacenamiento.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directa	**Electrónicos**

5.- Sitios de resguardo.

[redacted]

6.- Servidores públicos que tienen acceso a los sistemas de datos personales.

Titular de la Coordinación de Sistemas Informáticos, Titular de la Unidad de Transparencia y Jefe del Departamento de Comunicación.

7.- Encargado.

Proveedor/Tercero	No aplica
Actividad	
Relación	
Instrumento jurídico que formaliza la prestación del servicio	

8.- Transferencias que se realizan.

No se realizan transferencias a terceros.

9. Control archivístico.

Serie documental: No cuenta con serie documental.

Plazos de conservación: No hay plazos de conservación establecidos.

3.10 COORDINACIÓN DEL SISTEMA ESTATAL DE LA PNT

J.1- Sistema Infomex Sinaloa

1.- Servidor público responsable del sistema o base de tratamiento.

Titular de la Coordinación del Sistema Estatal de la Plataforma Nacional de Transparencia (PNT).

2.- Funciones y obligaciones de las personas que tratan datos personales.

Esta base de datos o sistema de tratamiento es para gestionar solicitudes de información y derechos ARCO de manera electrónica, (vía internet) para que cualquier persona pueda ejercer su derecho de acceso a la información pública, además de que permite a estos últimos cumplir cabalmente con sus atribuciones en materia de transparencia, derecho de acceso a la información pública y solicitud de datos personales.

La Coordinación Estatal de la PNT tiene funciones y obligaciones para realizar tratamiento de datos personales contenidos en esta base o sistema de tratamiento, con lo dispuesto en los artículos 27, 28 y 86 de la Ley de Transparencia, 63, 64, 65 y 72 de la LPDPPSOES.

3.- Datos personales que se recaban y su finalidad.

DATO PERSONAL	FINALIDAD
Nombre	**Principal:** Gestionar solicitudes de información de manera electrónica, (vía internet) para que cualquier persona pueda ejercer su derecho de acceso a la información pública y derechos ARCO.
Domicilio	
Correo electrónico	

Identificación oficial (Domicilio, sexo, fecha de nacimiento, fotografía y nacionalidad)	**Principal:** Acreditar la identidad cuando se ejerza alguno de los derechos ARCO.

4.- Forma de obtención y medios de almacenamiento.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directa	**Electrónicos**

5.- Sitios de resguardo.

[redacted]

6.- Servidores públicos que tienen acceso a los sistemas de datos personales.

Coordinador del Sistema Estatal de la Plataforma Nacional de Transparencia, quien tiene el acceso a la información y configuración de dicho sistema.

Mientras que los Comisionados, Secretarios Proyectistas, Analistas Jurídicos, Auxiliares Jurídicos de Ponencias, Director Jurídico Consultivo, Analistas Jurídicos adscritos a la Dirección Jurídica, Secretaria Ejecutiva y Analista Jurídico adscrito a la Secretaría Ejecutiva y Titular de la Unidad de Transparencia, solo tienen acceso a la información para consulta.

7.- Encargado.

Proveedor/Tercero	No aplica
Actividad	
Relación	
Instrumento jurídico que formaliza la prestación del servicio	

8.- Transferencias que se realizan.

No se realizan transferencias a terceros.

9.- Control archivístico.

Serie documental: No cuenta con serie documental.

Plazos de conservación: No cuenta con plazos de conservación.

J.2- Sistema SISAI

1.- Servidor público responsable del sistema o base de tratamiento.

Titular de la Coordinación del Sistema Estatal de la PNT.

2.- Funciones y obligaciones de las personas que tratan los datos personales.

Esta base de datos o sistema de tratamiento es con el fin de que los ciudadanos puedan realizar solicitudes de información o ejerza sus derechos ARCO.

La Coordinación Estatal de la PNT de la CEAIP tiene atribuciones para realizar tratamiento de datos personales contenidos en esta base o sistema de tratamiento, con lo dispuesto en los artículos 27, 28 y 86 de la Ley de Transparencia de Acceso a la Información Pública del Estado de Sinaloa.

3.- Datos personales que se recaban y su finalidad.

DATO PERSONAL	FINALIDAD
Nombre	**Principal:** Que los ciudadanos puedan realizar solicitudes de información o ejerza sus derechos ARCO en una sola Plataforma tecnológica .
Domicilio	
Correo electrónico	

4.- Forma de obtención y medios de almacenamiento.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directa	**Electrónicos**

5.- Sitios de resguardo.

[redacted]

6.- Servidores públicos que tienen acceso a los sistemas de datos personales.

Coordinador del Sistema Estatal de la Plataforma Nacional de Transparencia, quien tiene el acceso a la información y configuración de dicho sistema.

Mientras que los Comisionados, Secretarios Proyectistas, Analistas Jurídicos, Auxiliares Jurídicos de Ponencias, Director Jurídico Consultivo, Analistas Jurídicos adscritos a la Dirección Jurídica, Secretaria Ejecutiva y Analista Jurídico adscrito a la Secretaría Ejecutiva y Titular de la Unidad de Transparencia, solo tienen acceso a la información para consulta.

7.-Encargado.

Proveedor/Tercero	No aplica.
Actividad	
Relación	
Instrumento jurídico que formaliza la prestación del servicio	

8.- Transferencias que se realizan.

No se realizan transferencias a terceros.

9.- Control archivístico.

Serie documental: No cuenta con serie documental.

Plazos de conservación: No cuenta con plazos de conservación.

3.11 PONENCIAS DE LA CEAIP

K.1- Sistema de Recursos de Revisión.

1.- Servidor público responsable del área administrativa

Comisionadas y comisionados de la CEAIP.

2.- Funciones y obligaciones de las personas que tratan los datos personales.

Esta base de datos o sistema de tratamiento es con el fin de sustanciar y dictaminar la resolución correspondiente al recurso de revisión interpuesto ante la CEAIP al encontrarse el solicitante y/o recurrente inconforme con la respuesta emitida por los sujetos obligados, o bien en el supuesto de omisión a dar respuesta por parte del responsable, los cuales son tramitados por las Ponencias y posteriormente resueltos por el Pleno de la Comisión.

Las Ponencias de la CEAIP tiene atribuciones para realizar tratamiento de datos personales contenidos en esta base o sistema de tratamiento, con lo dispuesto en el artículo 32 fracción II, 170, 171 y 179 de la Ley; y 118 fracción IV de la LPDPPSOES; y 36 fracción IV y 37 del Reglamento Interior.

3.- Datos personales que se recaban y su finalidad.

DATO PERSONAL	FINALIDAD
Nombre	**Principal:** Requisito para el solicitante y/o recurrente al momento de interponer un recurso de revisión ante el sujeto obligado o directamente en la comisión.
Domicilio	**Principal:** Requisito para el solicitante y/o recurrente al momento de interponer un recurso de revisión ante el sujeto obligado o directamente en la comisión para efectos de oír y recibir notificaciones.
Correo electrónico	
Identificación oficial	**Principal:** Requisito para que el solicitante y/o recurrente al

	momento de interponer recurso de revisión en materia de datos personales, a fin de poder acreditar su identidad y, en su caso la personalidad de quien figura como representante.
Nombre del Sujeto Obligado	**Principal:** Para efectos de notificación al sujeto obligado.
Domicilio del Sujeto Obligado	
Correo electrónico institucional	

4.- Forma de obtención y medios de almacenamiento.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directa	**Físico:** Expedientes que contienen las actuaciones impresas de cada uno de los recursos de revisión, los cuales resguardan en un archivero. **Electrónico:** Se encuentran en la Plataforma Nacional de Transparencia.

5.- Sitios de resguardo.

[redacted]

6.- Servidores públicos que tienen acceso a los sistemas de datos personales.

Comisionadas (os), Secretarios (as) de Acuerdos y Proyectos, Analistas Jurídicos y Auxiliares Jurídicos de Ponencias. Una vez que se ordena el archivo del expediente el personal de la Secretaría Ejecutiva y Coordinación de Archivos, una vez que se realiza la transferencia primaria al Archivo de Concentración para su resguardo.

7.- Encargado.

Proveedor/Tercero	No aplica.
Actividad	
Relación	
Instrumento jurídico que formaliza la prestación del servicio	

8.- Transferencias que se realizan.

No se realizan transferencias a terceros.

9.- Control archivístico.

Serie documental: CEAIP.03.00.03.00

Plazos de conservación: Archivo de Trámite / 1 año – Archivo de Concentración / 5 años.

3.12 COORDINACIÓN DE ARCHIVOS

L.1- Sistema de Archivo de Concentración.

1.- Servidor público responsable del área administrativa

Coordinadora de Archivos y Jefe del Departamento de Archivos.

2.- Funciones y obligaciones de las personas que tratan los datos personales.

Esta base de datos o sistema de tratamiento es con el fin de asegurar y describir los fondos bajo su resguardo, así como la consulta de los expedientes; recibir las transferencias primarias y brindar servicios de préstamo y consulta a las unidades o áreas administrativas productoras de la documentación que resguarda; y conservar los expedientes hasta cumplir su vigencia documental de acuerdo con lo establecido en el catálogo de disposición documental; promover la baja documental de los expedientes que integran las series documentales que hayan cumplido su vigencia documental y, en su caso, plazos de conservación y que no posean valores históricos, conforme a las disposiciones jurídicas aplicables; e identificar los expedientes que integran las series documentales que hayan cumplido su vigencia documental y que cuenten

con valores históricos, y que serán transferidos a los archivos históricos según corresponda.

La Coordinación de Archivos tiene facultades y obligaciones para realizar tratamiento de datos personales contenidos en esta base o sistema de tratamiento, con lo dispuesto en el artículo 30 fracción I a la XI de la Ley de Archivos para el Estado de Sinaloa.

3.- Resguardan los datos personales contenidos en los sistemas siguientes:

A.1 Sistema de Expedientes del personal;

A.2 Sistema de procedimientos de contratación y pagos a proveedores;

A.3 Sistema de Recibos de nómina;

B.1 Auditorías, revisiones y visitas a las áreas (Informes de resultados);

B.2 Sistema de declaración de situación patrimonial, conflicto de intereses y constancia de presentación de declaración del ejercicio fiscal;

C.1 Sistema de Expedientes de solicitudes de información pública;

C.2. Sistema de solicitudes de ejercicio de derechos ARCO;

C.3 Sistema de asesorías;

C.4 Sistema de informes sobre seguimiento de resolución en carácter de sujeto obligado (DOT);

D.1 Procedimientos de Denuncias de Obligaciones de Transparencia;

D.3 Procedimientos Administrativos Sancionatorios;

E.1 Sistema de Ejecución de Cumplimientos e Incumplimientos;

G.1 Sistema de Registro de Capacitación para Sujetos Obligados;

G.2 Sistema de Registro de Socialización;

G.3 Sistema de Registro de Concursos y

K.1 Sistema de Recursos de Revisión.

4.- Forma de obtención y medios de almacenamiento.

FORMA DE OBTENCIÓN	MEDIOS DE ALMACENAMIENTO
Directa	**Electrónicos y físicos**

5.- Sitios de resguardo.

[redacted]

6.- Servidores públicos que tienen acceso a los sistemas de datos personales.

Coordinadora de Archivos y Jefe del Departamento de Archivos.

7.- Encargado.

Proveedor/Tercero	No aplica.
Actividad	
Relación	
Instrumento jurídico que formaliza la prestación del servicio	

8.- Transferencias que se realizan.

No se realizan transferencias a terceros.

9.- Control archivístico.

Serie documental: No cuenta.

Plazos de conservación: Cada expediente se resguarda hasta en tanto se cumpla con la vigencia y plazos de conservación respectivos, posteriormente se promueve la baja documental de los expedientes que integran las series documentales y que no posean valores históricos.

3.13 DIRECCIÓN DE VERIFICACIÓN Y SEGUIMIENTO

La Dirección de Verificación y Seguimiento de la CEAIP, no realiza tratamiento de datos personales de titulares.

3.14 DIRECCIÓN DE DATOS PERSONALES

La Dirección de Datos Personales, no realiza tratamiento de datos personales de titulares y únicamente tiene acceso al sistema D2, para apoyar en la sustanciación de los procedimientos de verificación en materia de datos personales.

4. MEDIDAS DE SEGURIDAD

De conformidad con los artículos 3, fracción XXI y 32 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y artículos 4, fracción XXVI y 41 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Sinaloa, las medidas de seguridad son el conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten proteger los datos personales.

Dichas medidas de seguridad deben ser adoptadas consideran el riesgo inherente a los datos personales tratados, la sensibilidad de los datos personales tratados, el desarrollo tecnológico, las posibles consecuencias de una vulneración para los titulares, las transferencias de datos personales que se realizan, el número de titulares, las vulneraciones previas ocurridas en los sistemas de tratamiento y el riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.

En ese sentido, el presente documento de seguridad establece las medidas de seguridad de carácter administrativas, técnicas y físicas que son implementadas al interior de la CEAIP, mismas que serán descritas a continuación:

MEDIDAS DE SEGURIDAD ADMINISTRATIVAS.

Las medidas de seguridad administrativas deben entenderse a las 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, por lo que al interior de la Comisión se cuentan con las siguientes:

Política/procedimiento	Descripción
MA.1 Guía de información confidencial.	Documento guía elaborado por la Dirección de Datos Personales para la Dirección de Administración de esta Comisión, el cual le permite identificar de manera más sencilla aquéllos datos de carácter confidencial por cada tipo de documento que maneja, con su respectiva fundamentación. Asimismo, en dicha guía se describe el procedimiento que debe seguir para aquéllos casos en los que aplique la clasificación de información para la elaboración de versiones públicas, ya sea para dar cumplimiento a una obligación de transparencia o atender una solicitud de información.
MA2. Lineamientos internos para el uso de videovigilancia en las instalaciones de la CEAIP.	Estos lineamientos elaborados por la Dirección de Datos Personales tienen por objeto establecer las bases, principios y procedimientos para el uso de videocámaras al interior de la Comisión, pues al recopilarse datos personales que hacen identificable a cualquier

	persona que se encuentre o circule por las instalaciones (imagen) resulta necesario garantizar la seguridad de los datos.
MA3. Protocolo para la Protección de Datos Personales en Documentos Físicos, Electrónicos y Digitales al interior de la CEAIP.	Documento elaborado por la Dirección de Datos Personales que establece medidas e instrucciones destinadas a garantizar la confidencialidad de la información tratada por las áreas de la Comisión, entre tales medidas e instrucciones se encuentra la de asegurar que los datos e información a los que tengan acceso solo se utilicen para las finalidades propios de las funciones de la Comisión; que solo el personal de cada área, en el ejercicio de sus funciones acceda a los datos personales; el establecimiento de contraseñas de acceso a los dispositivos de impresión; no dejar documentos impresos que contengan datos personales en la fotocopiadora; mantener las computadoras situadas de manera estratégica para que ningún tercero o servidor público no facultado observe datos personales, realizar periódicamente actualizaciones de seguridad en software, borrado seguro de información, entre otras.
MA4. Protocolo ante vulneraciones de datos personales.	Estos lineamientos elaborados por la Dirección de Datos Personales tienen por objeto establecer el procedimiento que debe seguirse por parte de los servidores públicos de la Comisión cuando se advierta que ocurrió una vulneración a la protección de los datos personales en su poder, entre los que se encuentra el

	registro de incidencias en la bitácora vulneraciones, la implementación de las medidas correctivas posibles, y la notificaciones a titulares y la CEAIP en su calidad de organismo garante cuando se hayan afectado de manera significativa derechos patrimoniales o morales de los titulares.
MA5. Programa General de Capacitación.	Plan de sensibilización y capacitación interna dirigida al personal de la CEAIP en materia de protección de datos personales, mismo que se encuentra definido en el numeral IX de este documento de seguridad.
MA6. Inventario de datos personales y sistemas de tratamiento.	Se realizó un inventario de los datos personales y sistemas de tratamiento de los mismos, respecto de la información confidencial que trata esta Comisión, el cual estará en constante actualización y se encuentra visible en el numeral II del presente documento de seguridad.

MEDIDAS DE SEGURIDAD FÍSICAS.

Las medidas de seguridad física son el conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento, mismas que de manera enunciativa más no limitativa, deben considerar actividades para a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información; b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información; c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y d) Proveer a los equipos que contienen o almacenan datos personales de un

mantenimiento eficaz, que asegure su disponibilidad e integridad. Dichas actividades se pueden llevar a cabo empleado o no la tecnología.

En tal virtud, la CEAIP ha implementado al interior de la institución las medidas de seguridad físicas siguientes:

Acción/mecanismo	Descripción/características
MF1. Tarjetas de acceso.	[redacted]
MF2. Oficinas privadas	[redacted]
MF3. Gavetas o archiveros.	[redacted]

MF4. Instalación de letreros.	
MF5. Detector de humo.	[redacted]
MF6. Extintores e hidratantes.	
MF7. Cámaras de seguridad.	
MF8. Registro de salida de equipos de cómputo y/o expedientes.	

MEDIDAS DE SEGURIDAD TÉCNICAS.

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.

Dichas medidas deben considerar el 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; generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones; revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware; y gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Por tal motivo y tomando en consideración que la CEAIP cuenta con equipo compuesto por hardware y software, a continuación se describen las diversas medidas técnicas con las que se cuenta:

Acción/mecanismo	Descripción/características
MT1. Usuario y contraseñas.	[redacted]
MT2. Antivirus.	

MT3. Copias de seguridad o respaldos de la información.	[redacted]
MT4. Formas de supresión y borrado seguro de información (electrónica).	
MT5. Mantenimiento de equipo.	[redacted]
MT6. Instalación y uso de software controlado.	
MT7. Firewall y DMZ	
MT8.Tickets	

5. ANÁLISIS DE RIESGOS

El análisis de riesgos considera la evaluación cuantitativa y cualitativa sobre la posibilidad de que un activo de información pueda sufrir una pérdida o daño. También contempla la identificación de activos, el estudio de causas y consecuencias de las amenazas y vulnerabilidades en los sistemas de tratamiento de datos personales, y permite establecer parámetros para ponderar los efectos de posibles vulneraciones de seguridad.

Es por ello que se realiza una clasificación de los datos personales a fin de poder ponderar el riesgo e identificar la información que por orden de prioridad requiera tener más protección.

Para poder darle un valor a los niveles de riesgo, se realizó el presente análisis en base a tres factores:

a) **Beneficio**, factor que deriva en el nivel de riesgo por tipo de dato, determinado por el riesgo inherente del dato y el volumen de titulares de las que se tratan datos.

b) **Accesibilidad**, factor que determina el nivel de riesgo por tipo de acceso, es decir, el número de accesos potenciales a los datos.

c) **Anonimidad**, factor que determina el nivel de riesgo por tipo de entorno desde el que se tiene acceso a los datos. Estos factores de riesgo nos permiten obtener un valor cuantitativo del nivel de riesgo latente de cada particular con relación al tratamiento de datos personales y sensibles y, a partir de ello, una lista de controles congruentes para disminuir los posibles impactos a los datos personales o sensibles.

Expuesto lo anterior, se ilustran las tablas realizadas por la CEAIP para elaborar el análisis de riesgo, así como el cuadro en el que se ilustra la matriz de análisis de riesgos de este organismo, lo anterior tomando como base la Metodología del Análisis de Riesgo BAA del INAI disponible el hipervínculo electrónico https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Metodolog%C3%ADa_de_An%C3%A1lisis_de_Riesgo_BAA(Junio2015).pdf.

Tipo de Dato	Riesgo Inherente	Nivel de Riesgo
Datos identificativos[1].	Bajo	1
Patrimoniales[2], académicos[3], jurídicos, procedimientos administrativos[4],	Medio	2

[1] **Datos identificativos**: El nombre, domicilio, teléfono particular, teléfono celular, firma, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), Matrícula del Servicio Militar Nacional, número de pasaporte, lugar y fecha de nacimiento, nacionalidad, edad, fotografía, demás análogos.

[2] **Datos patrimoniales:** Los correspondientes a bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, fianzas, servicios contratados, referencias personales, demás análogos

[3] **Datos académicos:** Trayectoria educativa, calificaciones, títulos, cédula profesional, certificados y reconocimientos.

[4] **Datos sobre procedimientos administrativos:** La información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio.

electrónicos[5] y laborales[6].		
Salud[7], biométricos[8], de tránsito y movimientos migratorios[9].	Alto	3
Origen étnico o racial, características morales o emocionales, ideología y opiniones políticas, creencias, convicciones religiosas, filosóficas y preferencia sexual, así como los datos de niños y niñas e información adicional de la tarjta bancaria[10].	Muy alto	4

En este punto, es necesario advertir que algunos tipos de datos de los que se mencionan son susceptibles de hacerse públicos, cuando por ley exista una obligación de difundirlos y/o se trate de servidores públicos, tal es el caso de algunos datos identificativos, patrimoniales, laborales, académicos, etcétera.

[5] **Datos electrónicos:** Las direcciones electrónicas, tales como, el correo electrónico no oficial, dirección IP (Protocolo de Internet), dirección MAC (dirección Media Access Control o dirección de control de acceso al medio), así como el nombre del usuario, contraseñas, firma electrónica; o cualquier otra información empleada por la persona, para su identificación en Internet u otra red de comunicaciones electrónicas;

[6] **Datos laborales:** Documentos de reclutamiento y selección, nombramiento, incidencia, capacitación, actividades extracurriculares, referencias laborales, referencias personales, solicitud de empleo, hoja de servicio.

[7] **Datos sobre la salud:** El expediente clínico de cualquier atención médica, referencias o descripción de sintomatologías, detección de enfermedades, incapacidades médicas, discapacidades, intervenciones quirúrgicas, vacunas, consumo de estupefacientes, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, así como el estado físico o mental de la persona.

[8] **Datos biométricos**: huellas dactilares, ADN, geometría de la mano, características de iris y retina.

[9] **Datos de tránsito y movimientos migratorios:** Información relativa al tránsito de las personas dentro y fuera del país, así como información migratoria.

[10] **Información adicional de la tarjeta bancaria:** cualquier otro dato relacionado o contenido en la misma, por ejemplo fecha de vencimiento, códigos de seguridad, datos de banda magnética o número de identificación personal (PIN).

Ahora bien, para identificar el nivel de riesgo por tipo de dato que se trata en la CEAIP, se suma el riesgo inherente más el volumen de titulares contenidos en la base de datos, por ejemplo.

- Menos de 500 titulares (>500), es decir de hasta 500 personas.
- Menos de 5,000 titulares (>5000), es decir de hasta 501 hasta 5,000;
- Menos de 50,000 (>50,000), es decir de hasta 5,001 hasta 50,000 personas; y
- Menos de 500,000 (<500,000), es decir, de 50, 001 hasta 500,000 personas.

De esta manera, visualizada en tabla queda de la siguiente manera:

Tipo de dato / Número de titulares	> 500	>5,000	>50,000	<500,000
Datos identificativos.	1	1	1	1
Datos Patrimoniales, académicos, jurídicos, procedimientos administrativos, electrónicos y laborales	1	1	2	3
Salud, biométricos, de tránsito y movimientos migratorios.	1	2	3	3
Origen étnico o racial, características morales o emocionales, ideología y opiniones políticas, creencias, convicciones religiosas, filosóficas y preferencia sexual, así como los datos de niños y niñas e información adicional de tarjeta bancaria.	4	4	4	4

El nivel de riesgo por tipo de dato sirve para determinar los controles que se deben considerar para su protección.

Una vez obtenido el factor beneficio, es decir el nivel de riesgo por tipo de dato, es necesario identificar el nivel de riesgo por tipo de acceso **(factor accesibilidad)**, este se realiza determinando la cantidad de accesos potenciales a los datos personales que se pretende proteger, es decir, definiendo cuántas personas tienen la posibilidad de acceder a la información en un intervalo de tiempo, por ejemplo, durante 24 horas. Para este parámetro, entre mayor sea la accesibilidad, mayor riesgo existe para la información.

Accesibilidad (Cantidad de accesos diarios a los datos personales).	**Nivel de Riesgo**
<20 (menos de 20)	1
>20 <200 (más de 20, menos de 200)	2
>200 <2,000 (más de 200, menos de 2,000)	3
>2,000 (más de 2,000)	4

Ahora bien, una vez obtenido el factor accesibilidad, identificamos el riesgo por tipo de entorno, este factor representa el nivel de anonimidad (**factor anonimidad**) para acceder o hacer uso de los datos personales que se tratan. Entre mayor anonimidad ofrezca el entorno, mayor riesgo existe de que se vulnere la seguridad. En caso de que se accedan por más de un entorno a los datos personales, se debe considerar el entorno de mayor riesgo.

Entorno	**Nivel de Riesgo**
Físico	1
Equipo de cómputo	2
Nube	3
Internet	4

Finalmente, es necesario señalar que para poder cuantificar el nivel del riesgo se utilizó la siguiente ecuación algebraica (a+b)*(c+d), la cual se puede interpretar como la sumatoria entre a) tipo de dato, más b)

volumen de los datos; **cuyo producto obtenido se multiplicara** por el por el resultado de la suma entre el c) accesibilidad más d) anonimidad.

El nivel de riesgo se calificará de la siguiente manera:

PUNTUACIÓN	NIVEL DE RIESGO
1-9	BAJO
10-15	MEDIO
16-20	ALTO
MÁS DE 21	MUY ALTO

MATRIZ ANÁLISIS DE RIESGOS						
Identificación			**Análisis**		**Evaluación**	
Sistema	Tipo de datos	Volumen	Accesibilidad	Anonimidad	Calificación	Nivel de riesgo
A.1	2	1	1	2	9	BAJO
A.2	2	1	1	2	9	BAJO
A.3	2	1	1	2	9	BAJO
A.4	1	1	1	2	6	BAJO
A.5	1	1	1	2	6	BAJO
B.1	2	1	1	1	6	BAJO
B.2	2	1	1	2	9	BAJO
C.1	1	1	1	2	6	BAJO
C.2	1	1	1	2	6	BAJO

C.3	1	1	1	2	6	BAJO
C.4	1	1	1	2	6	BAJO
D.1	1	1	1	2	6	BAJO
D.2	1	1	1	1	4	BAJO
D.3	1	1	1	1	4	BAJO
E.1	1	1	1	1	4	BAJO
F.1	1	1	1	2	6	BAJO
F.2	1	1	1	2	6	BAJO
G.1	1	1	1	2	6	BAJO
G.2	1	1	1	2	6	BAJO
G.3	4	1	1	2	15	MEDIO
G.4	1	1	1	2	6	BAJO
H.1	1	1	1	2	6	BAJO
H.2	1	1	1	2	6	BAJO
I.1	1	1	1	2	6	BAJO
I.2	1	1	1	2	6	BAJO
I.3	1	1	1	2	6	BAJO
I.4	1	1	1	2	6	BAJO
I.5	2	1	1	2	9	BAJO

I.6	1	1	1	2	9	BAJO
I.7	1	1	1	1	4	BAJO
J.1	1	1	1	2	6	BAJO
J.2	1	1	1	2	6	BAJO
K.1	1	1	1	2	6	BAJO
L.1	2	1	1	2	9	BAJO

Al realizar la identificación de activos, el estudio de causas y consecuencias de las posibles amenazas y vulnerabilidades que pueden presentarse en nuestros sistemas de tratamiento de datos personales se arrojó lo siguiente:

MATRIZ DE VULNERABILIDADES Y AMENAZAS								
Activo	**Vulnerabilidad**	**Amenaza**	**Consecuencias**	**Medida de seguridad para mitigar la amenaza**			**Potencial / Probabilidad**	
				Existe	**Insuficiente**	**No existe**	**Muy Probable**	**Poco Probable**
Hardware	Mantenimiento en los equipos insuficiente.	Falla en el sistema de datos.	Pérdida o daño.					
	Falta de un procedimiento para la sustitución de equipos.	Falla de equipos.	Pérdida o daño.					
	Susceptibilidad de daño físico.	Polvo, corrosión, congelamiento, fuego, agua, contaminación, radiación electromagnética.	Pérdida, destrucción o daño.					
	Falta de configuraciones adecuadas al equipo.	Falla en el funcionamiento del equipo.	Pérdida, destrucción, acceso o uso no autorizado.					
	Susceptibilidad a los cambios de voltaje.	Pérdida de suministro eléctrico.	Pérdida o destrucción.					
	Susceptible a las variaciones del ambiente.	Fenómenos meteorológicos.	Pérdida, destrucción o daño.					
	Almacenamiento no cifrado.	Robo de soportes electrónicos.	Robo, extravío o copia no autorizada/uso, acceso o tratamiento no autorizado.					
	Falta de cuidado en la destrucción de soportes electrónicos.	Robo de información y/o soportes.	Robo, extravío o copia no autorizada/uso, acceso o tratamiento no autorizado.					

Software	Falta de pruebas al software y su configuración.	Error en la operación de la aplicación	Daño, alteración o modificación.					
	Falta de actualizaciones de seguridad en software.	Abuso de derechos por parte de los usuarios.	Uso, acceso o tratamiento no autorizado.					
	No cerrar la sesión al abandonar la estación de trabajo.	Acceso no autorizado a los sistemas.	Uso, acceso o tratamiento no autorizado.					
	Desecho o reutilización de medios de almacenamiento sin un adecuado borrado seguro de información.	Consulta de información confidencial.	Robo, copia, uso, acceso o tratamiento no autorizado.					
	Falta de registros de auditoría.	Acciones fraudulentas.	Uso, acceso o tratamiento no autorizado.					
	Error en las asignaciones de derechos de acceso.	Intrusión en los sistemas.	Uso, acceso o tratamiento no autorizado.					
	Interfaces de usuario complicadas.	Error en la operación de los sistemas.	Uso, acceso o tratamiento no autorizado, daño, alteración o modificación.					
Redes	Falta de mecanismo de identificación y autenticación de usuario	Suplantación de identidad.	Pérdida, destrucción, robo, extravío o copia no autorizada, uso, acceso o tratamiento no autorizado.					
	Contraseñas no cifradas.	Intromisión y manipulación de los sistemas.	Pérdida, destrucción, robo, extravío o copia no					

			autorizada, uso, acceso o tratamiento no autorizado, daño alteración, modificación.					
	Servicios de red innecesarios habilitados y/o mal uso de protocolos.	Intrusión a la privacidad personal.	Uso, acceso o tratamiento no autorizado.					
	Falta de monitorización de los componentes de las redes, protocoles, servicios y aplicaciones.	Canales encubiertos y tráfico clandestino.	Uso, acceso, o tratamiento no autorizado.					
	Instalación y uso de software no contralado.	Ejecución de código malicioso.	Pérdida o destrucción, robo, extravío o copia no autorizada, uso, acceso o tratamiento no autorizado, daño, alteración o modificación de los datos.					
	Falta de respaldos.	Corrupción de datos en los sistemas.	Pérdida o destrucción, daño alteración o modificación.					
	Falta de un registro sobre la administración de los recursos.	Uso no autorizado de los servicios.	Robo, extravío o copia no autorizada, uso, acceso o tratamiento no autorizado.					
	Cableado de interconexión dañado o antiguo.	Malfuncionamiento en los equipos de telecomunicaciones.	Perdida, destrucción, robo, extravío o copia no					

			autorizada, uso, acceso o tratamiento no autorizado, daño, alteración o modificación.					
	Arquitectura de red insegura.	Espionaje o escucha de comunicaciones.	Robo, extravío o copia no autorizada, uso, acceso o tratamiento no autorizado					
	Líneas de comunicación sin protección.	Espionaje o escucha de comunicaciones.	Uso, acceso o tratamiento no autorizado					
Personal	Falta de personal sensibilizado y/o entrenado en seguridad.	Fraude y robo.	Uso, acceso o tratamiento no autorizado					
	Uso incorrecto de software y hardware.	Error en las operaciones de los sistemas.	Pérdida, destrucción, daño, alteración modificación.					
	Falta de supervisión al trabajo de externos.	Robo de información y/o soportes físicos/electrónicos	Pérdida o destrucción, robo, extravío o copia no autorizada, uso, acceso o tratamiento no autorizado, daño, alteración o modificación.					
	Falta de políticas acerca del uso de medios de telecomunicaciones.	Uso no autorizado de equipo.	Pérdida o destrucción, robo, extravío o copia no autorizada, uso, acceso o tratamiento no					

			autorizado, daño, alteración o modificación.					
Sitio/ SITE	Falta o implementación adecuada de controles de acceso.	Robo o destrucción de archivos.	Pérdida o destrucción, robo, extravío, o copia o autorizada, uso, acceso o tratamiento no autorizado, daño, alteración o modificación.					
	Lugar susceptible al daño por agua.	Inundaciones	Pérdida o destrucción.					
	Red eléctrica inestable.	Variación de voltaje	Pérdida o destrucción.					
Organización	Falta de procedimientos formales para la administración de derechos de usuario.	Abuso de privilegios por parte de los usuarios.	Pérdida o destrucción, robo, extravío, o copia o autorizada, uso, acceso o tratamiento no autorizado, daño, alteración o modificación.					
	Falta o ausencia de reporte de fallas.	Reincidencia de problemas.	Pérdida o destrucción, robo, extravío, o copia o autorizada, uso, acceso o tratamiento no autorizado, daño, alteración o modificación.					

	Falta de procedimiento formal para documentar y supervisar un SGSDP	Mal funcionamiento del SGSDP	Pérdida o destrucción, daño o alteración.					
	Falta de políticas de uso de correo electrónico	Fuga de información	Robo, extravío, copia no autorizada, uso, acceso o tratamiento no autorizado.					
	Falta de procedimientos para la instalación y actualización de los sistemas de información	Fallas en los sistemas de información.	Pérdida o destrucción, robo, extravío, o copia o autorizada, uso, acceso o tratamiento no autorizado, daño, alteración o modificación.					
	Falta de procesos estrictos en caso de un incidente o vulneración de seguridad	Malfuncionamiento del SGSDP	Pérdida o destrucción, robo, extravío, o copia o autorizada, uso, acceso o tratamiento no autorizado, daño, alteración o modificación					
	Falta de políticas para el uso de activos fuera de la organización	Robo de datos personales	Robo, extravío, copia no autorizada, uso, acceso o tratamiento no autorizado.					
	Falta de mecanismos de monitoreo para vulneraciones a la	Intrusión de personas malintencionadas	Pérdida o destrucción, robo, extravío, o copia o					

	seguridad de los datos.		autorizada, uso, acceso o tratamiento no autorizado, daño, alteración o modificación					
	Falta de procedimiento para reportar puntos débiles en la seguridad	Código malicioso	Pérdida o destrucción, robo, extravío, o copia o autorizada, uso, acceso o tratamiento no autorizado, daño, alteración o modificación					

6. ANÁLISIS DE BRECHA

Se realizó un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la CEAIP, a través de la aplicación del cuestionario "Medidas de seguridad existentes VS medidas de seguridad faltantes", cuyo contenido y resultados es el siguiente:

Análisis de Brecha			
(Medidas de seguridad existentes VS medidas de seguridad faltantes)			
Pregunta o Control	¿Existente?		
	SI	NO	Observaciones
Medidas de seguridad basadas en la cultura del personal			
¿Pones atención en no dejar a la vista información personal y llevas registro de su manejo?	26	1	
Política de escritorio limpio	24	3	
Hábitos de cierre y resguardo	23	4	
Impresoras, escáneres, copiadoras y buzones limpios	24	3	
¿Tienes mecanismos para eliminar de manera segura la información?	16	11	
Destrucción segura de documentos	16	11	
Eliminación segura de información en equipo de cómputo y medios de almacenamiento electrónico	17	10	
Fijar periodos de retención y destrucción de información	23	6	
Tomar precauciones con los procedimientos de re-utilización	24	3	

Informar al personal sobre sus deberes mínimos de seguridad y protección de datos	**10**	**17**	
Fomentar la cultura de la seguridad de la información	**16**	**11**	
Asegurar la protección de datos personales en subcontrataciones	**9**	**18**	
¿Tienes procedimientos para actuar ante vulneraciones a la seguridad de los datos personales?	**25**	**2**	
Tener un procedimiento de notificación	**7**	**20**	
¿Realizas respaldos periódicos de los datos personales?	**9**	**18**	
Medidas de seguridad en el entorno de trabajo físico			
¿Tienes medidas de seguridad para acceder al entorno de trabajo físico?	**31**	**0**	
Mantener registros del personal con acceso al entorno de trabajo	**11**	**16**	
¿Tienes medidas de seguridad para evitar el robo?	**17**	**10**	
Cerraduras y candados	**21**	**6**	
¿Cuidas el movimiento de información en entornos de trabajo físicos?	**23**	**4**	
Aprobación de salida de documentos, equipo de cómputo y/o medios de almacenamiento electrónico	**18**	**9**	
Mantener en movimiento sólo copias de la información, no el elemento original	**11**	**16**	
Usar mensajería certificada	**15**	**12**	

Medidas de seguridad en el entorno de trabajo digital			
¿Realizas actualizaciones al equipo de cómputo?	**20**	**7**	
¿Revisas periódicamente el software instalado en el equipo de cómputo?	**8**	**19**	
¿Tienes medidas de seguridad para acceder al entorno de trabajo electrónico?	**20**	**7**	
Uso de contraseñas y/o cifrado	**26**	**1**	
Bloqueo y cierre de sesiones	**22**	**5**	
Administrar usuarios y accesos	**18**	**9**	
¿Revisas la configuración de seguridad del equipo de cómputo?	**9**	**18**	
¿Tienes medidas de seguridad para navegar en entornos digitales?	**20**	**7**	
Reglas de navegación segura	**21**	**6**	
Uso de conexiones seguras	**25**	**2**	
¿Cuidas el movimiento de información en entornos de trabajo digitales?	**27**	**0**	

Seguridad de la información enviada y recibida	**24**	**3**	

Asimismo, se realizaron visitas in situ en cada una de las áreas administrativas que conforman la institución para efecto de constatar la información proporcionada.

Como resultado del cuestionario y de las visitas realizadas, se concluyó que **en general se tiene un nivel de medidas de seguridad óptimo en relación con los datos personales que se manejan**, tal como se desprende del listado de medidas de seguridad y de la matriz de vulnerabilidades y amenazas.

Sin embargo, de manera particular se detectaron algunas brechas que serán consideradas en el **Plan de Trabajo** para que las mismas sean cerradas, con el objetivo de mejorar la seguridad de los datos personales.

Área	Vulnerabilidad	Consecuencia
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]

7. PLAN DE TRABAJO

El plan de trabajo consiste en definir las acciones, medidas y métodos necesarios para implementar las **medidas de seguridad faltantes,** priorizando en todo momento las medidas de seguridad más relevantes e inmediatas a establecer, así como los recursos designados, el personal interno y externo en su organización y las fechas compromiso para la implementación de las medidas de seguridad nuevas o faltantes.

Por lo que el **Plan de Trabajo** a seguir quedará de la manera siguiente:

Medida de seguridad faltante	Acción/mecanismo	Área responsable	Periodo comprometido
[redacted]			

8. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Con la finalidad de supervisar el cumplimiento de las medidas de seguridad, se revisarán de manera periódica que éstas sean implementadas por los servidores públicos de la CEAIP, así como para asegurar que éstas cumplen con su objetivo de proteger los datos personales. Para ello la Dirección de Datos Personales llevará a cabo revisiones internas cada seis meses, levantando constancia de las mismas y enterando al Comité de Transparencia sobre el resultado de dichas previsiones.

9. PROGRAMA GENERAL DE CAPACITACIÓN

Con la finalidad de fortalecer la cultura de Protección de Datos Personales al interior de la CEAIP y actualizar de forma permanente a los servidores públicos con relación los sistemas de tratamiento a los cuales tienen acceso, la Dirección de Datos Personales desarrollará un Plan General de Capacitación, el cual se espera que genere un incremento y mejora en los niveles de seguridad de la CEAIP.

Tema	Periodo
"Documento de Seguridad y Vulneraciones de Datos Personales".	Primer trimestre
"Tratamiento de Datos Personales, principios y deberes".	Segundo trimestre
"Protección de Datos Personales en Documentos Físicos y Electrónicos de la CEAIP"	Cuarto trimestre

10. ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD

El presente documento será actualizado cuando ocurran los siguientes eventos:

1. Cuando se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;
2. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;
3. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad, e
4. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad; y
5. Cuando surjan documentos, formatos, recomendaciones, etc. por parte del INAI para la mejora del documento de seguridad.

11. DIRECTORIO

José Luis Moreno López
Comisionado Presidente

Liliana Margarita Campuzano Vega
Comisionada

José Alfredo Beltrán Estrada
Comisionado

Gustavo Reyes Garzón
Presidente del Comité de Transparencia y Director Jurídico Consultivo.

María Alejandra Gavilanez Gómez
Secretaria Técnica del Comité de Transparencia y Directora de Datos Personales.

Alfredo Atondo Quiñonez
Vocal del Comité de Transparencia y Director de Verificación y Seguimiento.

María de los Ángeles Acosta González
Analista Jurídico de la Dirección de Datos Personales

ANEXO 1

RELACIÓN DE SERVIDORES PÚBLICOS QUE TIENEN ACCESO A LOS SISTEMAS O BASE DE DATOS PERSONALES

Nombre	Área	Cargo	Sistema al que tiene acceso
Jorge Luis Rodríguez Cárdenas	Dirección de Administración	Director	A.1, A.2 y A.3
Leonel Jován Jiménez León	Dirección de Administración	Jefe del Departamento de Bienes y Suministros	A.2
Martha de Jesús Cárdenas Monjardín	Dirección de Administración	Analista Administrativo	A.1, A.2 y A.3
Alma Selene Ceballos Padilla	Dirección de Administración	Analista	A.1, A.2 y A.3
José Miguel Alarcón Barrios	Dirección de Administración	Analista Administrativo	A.1, A.2 y A.3
Gerardo Luis Mercado Ponce	Dirección de Administración	Analista de Planeación	No tiene acceso
José Luis Sandoval Gutiérrez	Dirección de Administración	Analista de Planeación Institucional	No tiene acceso
Hussien Badwan Paez	Dirección de Administración	Analista	No tiene acceso
Acéfalo	Órgano Interno de Control	Titular del Órgano Interno de Control	B.1 y B.2
Rafael Vega Gutiérrez	Órgano Interno de Control	Jefe del Departamento de Investigación	B.1 y B.2
Acéfalo	Órgano Interno de Control	Analista	B.1 y B.2
Sofía Karely Molina Espinoza	Unidad de Transparencia	Titular de la Unidad de Transparencia	C.1, C.2, C.3, C.4 e I.7

Gustavo Reyes Garzón	Dirección Jurídica Consultiva	Director	D.1, D.2, D.3, J.1 y J.2
Osiris Aleyda Beltrán Angulo	Dirección Jurídica Consultiva	Analista Jurídico	D.1, D.2 y D.3
Alán Alfonso Pérez Ramos	Dirección Jurídica Consultiva	Analista Jurídico	D.1, D.2 y D.3
Carlos Roberto Martínez Soto	Dirección Jurídica Consultiva	Analista notificador	D.1, D.2 y D.3
José Carlos Ávila Ortega	Dirección Jurídica Consultiva	Analista notificador	D.1, D.2 y D.3
Ana Cristina Félix Franco	Secretaría Ejecutiva	Secretaria Ejecutiva	E.1, J.1 y J.2
Martha Alicia Camarena Urías	Secretaría Ejecutiva	Titular de la Oficialía de Partes	No tiene acceso
Fredy Nampulá Trujillo	Secretaría Ejecutiva	Analista Jurídico	E.1
Genoveva Bejarano Espinoza	Secretaría Ejecutiva	Analista	E.1
Stephanie Clarisa Mendoza Medina	Secretaría Ejecutiva	Recepcionista	No tiene acceso
Gabriel Ernesto Mercado Guerrero	Gobierno Abierto	Titular de Gobierno Abierto	F.1 y F.2
Pablo Rocha Moraga	Dirección de Capacitación y Vinculación Ciudadana	Director	G.1, G.2, G.3, G.4 e I.1
Fabiola Valle Sánchez	Dirección de Capacitación y Vinculación Ciudadana	Jefa del Departamento de Vinculación	G.1, G.2, G.3, G.4 e I.1
Mario Antonio Millán Sarabia	Departamento de Comunicación	Jefe del Departamento de Comunicación	H.1 e I.7

Fermín II Rosas Quezada	Departamento de Comunicación	Analista de Diseño	H.2
Angela Consuelo Torres Ortiz	Departamento de Comunicación	Analista	No tiene acceso
Christian Norhel Ramírez Escobar	Coordinación de Sistemas Informáticos	Coordinador	I.1, I.2, I.3, I.4, I.5, I.6, e I.7.
Sindy Yarely Inzunza Ruelas	Coordinación de Sistemas Informáticos	Analista	I.1, I.3 e I.6
Jesús Jaime Barraza Lizárraga	Coordinación de la Plataforma Nacional de Transparencia	Coordinador	J.1 y J.2
José Luis Moreno López	Ponencia	Comisionado Presidente	E.1, I.4, J.1, J.2 y K.1
Liliana Margarita Campuzano Vega	Ponencia	Comisionada	E1, I4, J1, J2 y K1
José Alfredo Beltrán Estrada	Ponencia	Comisionada	E.1, I.4, J.1, J.2
Eliane Gastelum Camacho	Ponencia	Secretaria de Acuerdos y Proyectos	E.1, J.1, J.2 y K.1
Emmanuel Dueñas Peña	Ponencia	Secretaria de Acuerdos y Proyectos	E.1, J.1, J.2 y K.1
Teresita Castro Aguilasocho	Ponencia	Secretaria de Acuerdos y Proyectos	E.1, J.1, J.2 y K.1
Andrea Villaverde Molina	Ponencia	Analista Jurídico	E.1, J.1, J.2 y K.1
Lailen Lapizco Peiro	Ponencia	Analista Jurídico	E.1, J.1, J.2 y K.1
Maykel Rodríguez Bustamante	Ponencia	Analista Jurídico	E.1, J.1, J.2 y K.1
María de Jesús Sandoval Obeso	Ponencia	Analista	E.1, J.1, J.2 y K.1
Nubia Valenzuela Pérez	Ponencia	Analista	E.1, J.1, J.2 y K.1
Juan Carlos Calderón Coronel	Ponencia	Auxiliar	E.1, J.1, J.2 y K.1

Héctor Alejandro Corralez Bejarano	Ponencia	Auxiliar	E.1, J.1, J.2 y K.1
Margarita Zambrano	Coordinación de Archivos	Coordinadora	A.1, A.2, A.3, B.1, B.2, C.1, C.2, C.3, C.4, D.1, E.1, G.1, G.2, G.3, y K.1 solo tiene acceso hasta que se realiza la transferencia primaria al archivo de concentración.
José Abelardo Félix Mariscal	Coordinación de Archivos	Jefe del Departamento de Archivos	A.1, A.2, A.3, B.1, B.2, C.1, C.2, C.3, C.4, D.1, E.1, G.1, G.2, G.3, y K.1 solo tiene acceso hasta que se realiza la transferencia primaria al archivo de concentración.
María Alejandra Gavilanez Gómez	Dirección de Datos Personales	Directora	D.2

ANEXO 2

ENCARGADOS DE DATOS PERSONALES

Sistema	Proveedor/Tercero	Actividad	Relación	Instrumento jurídico que formaliza la prestación del servicio.
A.3	Chávez Amez y Compañía S.C.	Auditoría de estados financieros 2021 y 2022	Contratación de servicios profesionales	Contrato de prestación de servicios profesionales
I.2	SITEGROUND	Servicio de alojamiento web	Proveedor de servicio de hosting	Contrato que establece términos y condiciones del servicio
I.3	SITEGROUND	Servicio de alojamiento web	Proveedor de servicio de hosting	Contrato que establece términos y condiciones del servicio

ANEXO 3

CONTROL DE VERSIONES Y/O ACTUALIZACIONES

Versión	Descripción	Fecha
1.0	Creación del Documento	Creado en 2022, aprobado por el Comité de Transparencia el 8 de marzo de 2023