ceaip
Comisión Estatal para el Acceso a la Información Pública
SINALOA

**OFICIO NO. CEAIP-DDP/029/2024**
**Asunto:** Respuesta solicitud de información 250486200012624

Culiacán, Sinaloa, a 15 de octubre de 2024.

**Lic. Maykel Rodríguez Bustamante**
**Jefa de la Unidad de Transparencia**
**Presente.**

De conformidad con lo dispuesto en el artículo 136 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Sinaloa (LTAIPES), dando atención al objeto de la solicitud de información folio **250486200012624**, la que fue formalmente presentada ante esta Comisión el día 23 de septiembre de 2024, al respecto y con el propósito de atender su petición y garantizar en todo momento el efectivo derecho consagrado en el artículo 6°, apartado A, de la Constitución Política de los Estados Unidos Mexicanos, me permito comunicarle lo siguiente.

A través de la solicitud en comento, se requirió a esta Dirección de Datos Personales, mediante escrito de fecha 26 de septiembre de 2024, emitido de su parte como Jefa de la Unidad de Transparencia, dar respuesta a los siguientes cuestionamientos:

> *"Se me informe qué políticas en materia de protección de datos personales han diseñado y/o implementado.*
>
> *Se me entregue el documento de seguridad.*
>
> *Qué medidas de seguridad han adoptado para mantener exactos, completos, correcto y actualizados los datos personales. ?*
>
> *Qué procedimientos han establecidos para la conservación y en su caso, bloqueo y supresión de los datos personales. ?*
>
> *Qué procedimientos han implementado y/o desarrollado para recibir y responder dudas y quejas de los titulares de los datos personales y en que consiste?*
>
> *Qué mecanismos han utilizados y/o aplicados para cumplir con los plazos fijados para la supresión de los datos personales?*
>
> *En los años 2010 a la fecha que mecanismos y/o desarrollado han aplicado para la revisión periódica sobre la necesidad de conservar los datos personales y cuáles son.?*

ceaip
Comisión Estatal para el Acceso a la Información Pública
SINALOA

*Qué códigos de buenas prácticas y/o modelo en materia de protección de datos personales han implementado y/o realizado y/o elaborado ect.*

*Qué programas y/o políticas de protección de datos personales han implementado y/o realizado y/o elaborado ect.*

*Qué programas y/o políticas de seguridad de datos personales han implementado en su institución y/o dependencia de los años 2023 y 2024 y cuáles son?*
*Qué programas y/o servicios y/o sistemas y/o plataformas informáticas han realizado y/o implementado y/o diseñado para el tratamiento de los datos personales. ?*

*Qué medidas de seguridad han implementado para mantener la seguridad para la protección de los datos personales que permitan protegerlo contra daño, y/o pérdida y/o alteración y/o destrucción para garantizar su confidencialidad, integridad y disponibilidad.*

*Se me entregué en copia escaneada de la bitácora de las vulneraciones de seguridad que han tenido sobre los tratamientos de los datos personales.*

*Cuántos casos de vulneración han reportado al órgano garante sobre la vulneraciones de los datos personales en los años de 2010 a la fecha.*

*Qué mecanismos y/o controles han implementado y/o realizado sobre aquellas personas y/o servidores públicos que intervengan para garantizar y guardar la confidencialidad sobre los datos personales que utilizan en sus tratamientos de los datos personales.*

*Cuántas personales y/o servidores públicos manejan datos personales se me informen por su nombre de los servidores públicos, área de adscripción y el cargo.*

*Copia escaneada del nombramiento de su oficial de protección de datos personales.*

*Cuántas transferencias han realizado en materia de datos personales en este año 2024.*

*Cuentan con el Programa Integral de Gestión de Datos, en caso de contar con dicho programa se me proporcione.*

*Qué mecanismos han implementado y/o realizado para asegurar que los datos personales se entregue solo a sus titulares y/o representantes.*

*Cuántas auditorías en materia de datos personales han realizado a los sujetos obligados desde el 2010 a la fecha y cuáles son esos sujetos obligados.*

*Se me explique cuáles son las medidas que aplican para uno de los principios incorporados en la LGPDPPSO, para garantizar el tratamiento de los datos personales*
.

*Qué sujetos obligados han presentado su evaluación de impacto en la protección de datos personales en los años 2020 a la fecha.*

*Cuantas recomendaciones no vinculantes han emitido sobre el contenido de la evaluación de impacto de los años 2020 a la fecha." [sic]*

Por lo que, en relación a los elementos informativos antes precisados, se responde lo siguiente:

1. ***"Se me informe qué políticas en materia de protección de datos personales han diseñado y/o implementado."***

En respuesta a la pregunta que se contesta, se informa que se han diseñado y/o implementado las siguientes:

- Guía de Información Confidencial de la Dirección de Administración de la CEAIP.
- Lineamientos Internos para el uso de videovigilancia en las instalaciones de la Comisión Estatal para el Acceso a la Información Pública.
- Protocolo ante las vulneraciones de datos personales.
- Protocolo para la Protección de datos personales en documentos físicos, electrónicos y digitales al interior de la CEAIP.
- Bitácora de Vulneraciones.
- Formato de Registro de Salida de Soportes Físicos.
- Lineamientos para la recepción de documentos del personal de la CEAIP y llenado de la Ficha curricular.
- Compromiso de confidencialidad.

2. ***"Se me entregue el documento de seguridad."***

En respuesta a la pregunta que se contesta, se anexa en versión pública el Documento de Seguridad solicitado, así como la correspondiente resolución del Comité de Transparencia, por la que se confirma la clasificación parcial de la información solicitada, ya que contiene información de carácter reservada conforme lo establecido en la Ley de Transparencia y Acceso a la Información Pública del Estado de Sinaloa.

3. ***"Qué medidas de seguridad han adoptado para mantener exactos, completos, correcto y actualizados los datos personales.?"***

Al respecto, se informa que esta Comisión cuenta con las siguientes medidas de seguridad en materia de datos personales relativas al objeto de la solicitud de información:

ceaip
Comisión Estatal para el Acceso a la Información Pública
SINALOA

**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:

- Guía de información confidencial.
- Lineamientos internos para el uso de videovigilancia en las instalaciones de la CEAIP.
- Protocolo para la Protección de Datos Personales en Documentos Físicos, Electrónicos y Digitales al interior de la CEAIP.
- Protocolo ante vulneraciones de datos personales.
- Programa General de Capacitación.
- Inventario de datos personales y sistemas de tratamiento.

**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 empleando o no la tecnología.

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

- Acceso regulado mediante credenciales electrónicas personales
- Oficinas privadas
- Gavetas o archiveros.
- Señalización de acceso restringido
- Detector de humo.
- Extintores.
- Cámaras de seguridad.
- Registro de salida de equipos de cómputo y/o dispositivos electrónicos.

**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:

- Usuario y contraseñas.
- Antivirus.
- Copias de seguridad o respaldos de la información.
- Formas de supresión y borrado seguro de información (electrónica).
- Mantenimiento de equipo.
- Instalación y uso de software controlado.
- Firewall y DMZ
- Tickets para atención de información en la Plataforma Nacional de Transparencia.

4. ***"Qué procedimientos han establecidos para la conservación y en su caso, bloqueo y supresión de los datos personales.?"***

En relación a los procedimientos para la conservación y en su caso borrado seguro de datos personales, se cuenta con el *Protocolo para la Protección de datos personales en documentos físicos, electrónicos y digitales al interior de la CEAIP,* así como los lineamientos emitidos por el Sistema Nacional de Transparencia respecto a la conservación y eliminación de archivos.

Así, en relación al borrado seguro de la información, dicho protocolo señala que una vez que concluya el plazo de conservación de los archivos físicos y electrónicos que contienen datos personales **se deben suprimir mediante la baja archivística**.

En todo momento los plazos de conservación atenderán las finalidades concretas, explicitas, licitas y legítimas previstas en el aviso de privacidad y que motivaron el tratamiento.

Los plazos de conservación de los datos personales no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron su tratamiento, y deberán atender a las disposiciones aplicables en la materia de que se trate y considerar los aspectos administrativos, contables, fiscales, jurídicos e históricos de los datos personales.

Para evitar la continuación en el tratamiento de datos personales cuya vigencia o finalidades han sido cumplidas, una vez realizadas las transferencias primarias al archivo de concentración, el área productora **procederá a la eliminación integral de datos personales en la base de datos que corresponda**, para asegurar que dichos archivos dejen de estar disponibles.

En el caso de la información electrónica, para su eliminación, se deberán utilizar los programas de informática utilizados por la Coordinación de Sistemas Informáticos.

Es menester señalar que, en relación a la conservación de datos personales, se observa lo previsto en la Ley de Archivos para el Estado de Sinaloa, y todos los sistemas de tratamiento por área administrativa cuentan con plazos de conservación definidos respecto de las series documentales que obran en su poder, conforme lo señalado en el documento de seguridad que se anexa a la respuesta.

5. ***"Qué procedimientos han implementado y/o desarrollado para recibir y responder dudas y quejas de los titulares de los datos personales y en qué consiste?"***

Esta Dirección de Datos Personales cuenta con un modelo de atención para recibir y responder dudas y/o quejas en materia de datos personales, a través de los diferentes medios electrónicos y digitales, como lo son por llamada telefónica y/o correo electrónico; asimismo se atiende a particulares y/o servidor o servidora pública de manera presencial.

La atención se realiza de acuerdo a la manera en que la asesoría haya sido requerida, una vez atendido el requerimiento, la información se registra en una base de datos donde se contempla la siguiente información: Fecha, indicar si fue requerida por un Sujeto Obligado o particular, vía/medio de contacto, folio de la solicitud/recurso, tema y observaciones.

Cabe señalar que, en relación a la atención de quejas de los titulares de datos personales, en caso de consistir en una vulneración en el tratamiento de sus datos personales, se insta a la persona titular a ejercer su derecho de denuncia si considera que ha sido afectado por actos del responsable que puedan ser contrarios a lo dispuesto por la Ley de Protección de Datos Personales en Posesión de Sujetos Obligado del Estado de Sinaloa y demás normativa aplicable, conforme lo estipulado en los artículos 158 fracción II, 159 y demás correlativos del primer ordenamiento citado.

6. ***"Qué mecanismos han utilizados y/o aplicados para cumplir con los plazos fijados para la supresión de los datos personales?"***

En relación a la pregunta que se contesta, es importante precisar que, cada área responsable del tratamiento de datos personales dentro de esta Comisión, es la responsable de realizar una revisión periódica sobre la necesidad de conservar los datos personales que obren en su poder, de conformidad con lo establecido en el los artículos 24, 25 y 26 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligado del Estado de Sinaloa; así como que, queda a salvo la facultad de las y los titulares de los datos personales para ejercer sus derechos de cancelación y oposición.

Así, esta Comisión cuenta un *Protocolo para la Protección de datos personales en documentos físicos, electrónicos y digitales al interior de la CEAIP*, en el que se señala que **una vez que concluya el plazo de conservación** de los archivos físicos y electrónicos que contienen datos personales se deben suprimir mediante la baja archivística; asimismo, en todo momento **los plazos de conservación** atenderán las finalidades concretas, explicitas, licitas y legítimas previstas en el aviso de privacidad y que motivaron el tratamiento.

**Los plazos de conservación** de los datos personales no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron su tratamiento, y deberán atender a las disposiciones aplicables en la materia de que se trate y considerar los aspectos administrativos, contables, fiscales, jurídicos e históricos de los datos personales.

7. ***"En los años 2010 a la fecha que mecanismos y/o desarrollado han aplicado para la revisión periódica sobre la necesidad de conservar los datos personales y cuáles son.?"***

En relación a la pregunta que se contesta, es importante precisar que, cada área responsable del tratamiento de datos personales dentro de esta Comisión, es la responsable de realizar una revisión periódica sobre la necesidad de conservar los datos personales que obren en su poder, de conformidad con lo establecido en el los artículos 24, 25 y 26 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligado del Estado de Sinaloa.

Así, en relación a los procedimientos para la revisión periódica sobre la necesidad de conservar los datos personales, esta Comisión cuenta el siguiente protocolo:

- Protocolo para la Protección de datos personales en documentos físicos, electrónicos y digitales al interior de la CEAIP.

8. ***"Qué códigos de buenas prácticas y/o modelo en materia de protección de datos personales han implementado y/o realizado y/o elaborado ect."***

En respuesta a la pregunta que se contesta, se informa que se han implementado y/o realizado y/o elaborado los siguientes modelos en materia de protección de datos personales:

- Guía de Información Confidencial de la Dirección de Administración de la CEAIP.
- Lineamientos Internos para el uso de videovigilancia en las instalaciones de la Comisión Estatal para el Acceso a la Información Pública.
- Protocolo ante las vulneraciones de datos personales.
- Protocolo para la Protección de datos personales en documentos físicos, electrónicos y digitales al interior de la Ceaip.
- Bitácora de Vulneraciones.
- Formato de Registro de Salida de Soportes Físicos.
- Lineamientos para la recepción de documentos del personal de la CEAIP y llenado de la Ficha curricular.
- Compromiso de confidencialidad.

9. ***"Qué programas y/o políticas de protección de datos personales han implementado y/o realizado y/o elaborado ect."***

En respuesta a la pregunta que se contesta, se informa que se han implementado y/o realizado y/o elaborado los siguientes programas y/o políticas de protección de datos personales:

- Guía de Información Confidencial de la Dirección de Administración de la CEAIP.
- Lineamientos Internos para el uso de videovigilancia en las instalaciones de la Comisión Estatal para el Acceso a la Información Pública.
- Protocolo ante las vulneraciones de datos personales.
- Protocolo para la Protección de datos personales en documentos físicos, electrónicos y digitales al interior de la CEAIP.
- Bitácora de Vulneraciones.
- Formato de Registro de Salida de Soportes Físicos.
- Lineamientos para la recepción de documentos del personal de la CEAIP y llenado de la Ficha curricular.
- Compromiso de confidencialidad.

10. ***"Qué programas y/o políticas de seguridad de datos personales han implementado en su institución y/o dependencia de los años 2023 y 2024 y cuáles son?"***

En respuesta a la pregunta que se contesta, se informa que durante los años 2023 y 2024 se han diseñado y/o implementado los siguientes programas y/o políticas de seguridad de datos personales:

- Guía de Información Confidencial de la Dirección de Administración de la CEAIP.
- Lineamientos Internos para el uso de videovigilancia en las instalaciones de la Comisión Estatal para el Acceso a la Información Pública.
- Protocolo ante las vulneraciones de datos personales.
- Protocolo para la Protección de datos personales en documentos físicos, electrónicos y digitales al interior de la CEAIP.
- Bitácora de Vulneraciones.
- Formato de Registro de Salida de Soportes Físicos.
- Lineamientos para la recepción de documentos del personal de la CEAIP y llenado de la Ficha curricular.
- Compromiso de confidencialidad.

11. ***"Qué programas y/o servicios y/o sistemas y/o plataformas informáticas han realizado y/o implementado y/o diseñado para el tratamiento de los datos personales.?"***

En respuesta a la pregunta que se contesta, se informa que la cantidad de la información requerida es 0 (cero).

No obstante lo anterior, se comunica que se encuentra en proceso de diseño una plataforma informática para el tratamiento de datos personales.

12. ***"Qué medidas de seguridad han implementado para mantener la seguridad para la protección de los datos personales que permitan protegerlo contra daño, y/o pérdida y/o alteración y/o destrucción para garantizar su confidencialidad, integridad y disponibilidad."***

En respuesta a la pregunta que se contesta, se informa que esta Comisión ha implementado las siguientes medidas de seguridad para la protección de datos personales, contra daño y/o pérdida y/o alteración y/o destrucción, así como para garantizar su confidencialidad, integridad y disponibilidad:

ceaip
Comisión Estatal para el Acceso a la Información Pública
SINALOA

**a) 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:

- Guía de información confidencial.
- Lineamientos internos para el uso de videovigilancia en las instalaciones de la CEAIP.
- Protocolo para la Protección de Datos Personales en Documentos Físicos, Electrónicos y Digitales al interior de la CEAIP.
- Protocolo ante vulneraciones de datos personales.
- Programa General de Capacitación.
- Inventario de datos personales y sistemas de tratamiento.

**b) 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:

- Acceso regulado mediante credenciales electrónicas personales
- Oficinas privadas
- Gavetas o archiveros.
- Señalización de acceso restringido
- Detector de humo.
- Extintores.
- Cámaras de seguridad.
- Registro de salida de equipos de cómputo y/o dispositivos electrónicos.

**c) 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:

- Usuario y contraseñas.
- Antivirus.
- Copias de seguridad o respaldos de la información.
- Formas de supresión y borrado seguro de información (electrónica).
- Mantenimiento de equipo.
- Instalación y uso de software controlado.
- Firewall y DMZ.
- Tickets para atención de información en la Plataforma Nacional de Transparencia.

***13. "Se me entregué en copia escaneada de la bitácora de las vulneraciones de seguridad que han tenido sobre los tratamientos de los datos personales."***

En respuesta a la pregunta que se contesta, se anexa en archivo digital el formato de Bitácora de Vulneraciones; asimismo, en virtud de que, la persona solicitante no señaló el periodo respecto del que requiere la información; se hace de su conocimiento que, durante el último año, es decir del 23 de septiembre de 2023 al 23 de septiembre de 2024, fecha esta última de su solicitud de información, no se han registrado vulneraciones de seguridad, por lo que, dichas vulneraciones son igual a 0 (cero).

14. **"Cuántos casos de vulneración han reportado al órgano garante sobre la vulneraciones de los datos personales en los años de 2010 a la fecha."**

En respuesta a la pregunta que se contesta, se hace de su conocimiento que, del año 2010 al 23 de septiembre de 2024, fecha de presentación de la solicitud de información, se ha reportado 01 caso a este organismo garante sobre la vulneración de datos personales.

15. ***"Qué mecanismos y/o controles han implementado y/o realizado sobre aquellas personas y/o servidores públicos que intervengan para garantizar y guardar la confidencialidad sobre los datos personales que utilizan en sus tratamientos de los datos personales."***

En respuesta a la pregunta que se contesta, se hace de su conocimiento que, mediante Acuerdo AP-CEAIP 29/2023, el Pleno de esta Comisión aprobó la implementación del "Compromiso de Confidencialidad por parte de las y los Servidores Públicos de la CEAIP", como mecanismo que tiene por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales, guarden confidencialidad respecto a éstos; se anexa a la presente respuesta el acuerdo citado.

16. ***"Cuántas personales y/o servidores públicos manejan datos personales se me informen por su nombre de los servidores públicos, área de adscripción y el cargo."***

En respuesta a la pregunta que se contesta, se proporciona la relación del personal que, a la fecha de la respuesta y de conformidad con el inventario de datos personales y de los sistemas de tratamiento por área administrativa señalados en el documento de seguridad de esta Comisión, manejan datos personales; así como, el área de adscripción y cargo que ostentan; siendo un total de 35 servidoras y servidores públicos.

| | Nombre | Área | Cargo |
|---|---|---|---|
| 1 | Jorge Luis Rodríguez Cárdenas | Dirección de Administración | Director |
| 2 | Leonel Jován Jiménez León | Dirección de Administración | Jefe del Departamento de Bienes y Suministros |

| | | | |
|---|---|---|---|
| 3 | Martha de Jesús Cárdenas Monjardín | Dirección de Administración | Analista Administrativo |
| 4 | Alma Selene Ceballos Padilla | Dirección de Administración | Analista |
| 5 | José Miguel Alarcón Barrios | Dirección de Administración | Analista Administrativo |
| 6 | Ana Cecilia García Navarro | Órgano Interno de Control | Titular del Órgano Interno de Control |
| 7 | Margarita Payán Quiroz | Órgano Interno de Control | Jefe del Departamento de Investigación |
| 8 | Maykel Rodríguez Bustamante | Unidad de Transparencia | Titular de la Unidad de Transparencia |
| 9 | María Alejandra Gavilánez Gómez | Dirección Jurídica Consultiva | Directora |
| 10 | Osiris Aleyda Beltrán Angulo | Dirección Jurídica Consultiva | Analista Jurídico |
| 11 | Alán Alfonso Pérez Ramos | Dirección Jurídica Consultiva | Analista Jurídico |
| 12 | Carlos Roberto Martínez Soto | Dirección Jurídica Consultiva | Analista notificador |
| 13 | José Carlos Ávila Ortega | Dirección Jurídica Consultiva | Analista notificador |
| 14 | Gustavo Reyes Garzón | Secretaría Ejecutiva | Secretario Ejecutivo |
| 15 | Fredy Nampulá Trujillo | Secretaría Ejecutiva | Analista Jurídico |
| 16 | Genoveva Bejarano Espinoza | Secretaría Ejecutiva | Analista |
| 17 | Pablo Rocha Moraga | Dirección de Capacitación y | Director |

| | | | |
|---|---|---|---|
| | | Vinculación Ciudadana | |
| 18 | Fabiola Valle Sánchez | Dirección de Capacitación y Vinculación Ciudadana | Jefa del Departamento de Vinculación |
| 19 | Mario Antonio Millán Sarabia | Departamento de Comunicación | Jefe del Departamento de Comunicación |
| 20 | Fermín II Rosas Quezada | Departamento de Comunicación | Analista de Diseño |
| 21 | Christian Norhel Ramírez Escobar | Coordinación de Sistemas Informáticos | Coordinador de Sistemas Informáticos |
| 22 | Sindy Yarely Inzunza Ruelas | Coordinación de Sistemas Informáticos | Analista de Sistemas |
| 23 | Jesús Jaime Barraza Lizárraga | Coordinación de la Plataforma Nacional de Transparencia | Coordinador Estatal de la Plataforma Nacional de Transparencia |
| 24 | José Luis Moreno López | Ponencia | Comisionado |
| 25 | Liliana Margarita Campuzano Vega | Ponencia | Comisionada |
| 26 | José Alfredo Beltrán Estrada | Ponencia | Comisionada |
| 27 | Eliane Gastelum Camacho | Ponencia | Secretaria de Acuerdos y Proyectos |
| 28 | Emmanuel Dueñas Peña | Ponencia | Secretaria de Acuerdos y Proyectos |
| 29 | Lailen Lapizco Peiro | Ponencia | Secretaria de Acuerdos y Proyectos |
| 30 | Andrea Villaverde Molina | Ponencia | Analista Jurídico |

| | | | |
|---|---|---|---|
| 31 | Gemma Marlen Nunfio León | Ponencia | Analista de Ponencia |
| 32 | María de Jesús Sandoval Obeso | Ponencia | Analista |
| 33 | Juan Carlos Calderón Coronel | Ponencia | Auxiliar |
| 34 | Margarita Zambrano | Coordinación de Archivos | Coordinadora |
| 35 | Teresita Castro Aguilasocho | Dirección de Datos Personales | Directora |

***17. "Copia escaneada del nombramiento de su oficial de protección de datos personales."***

En relación a la pregunta que se contesta, se hace de su conocimiento que en esta Comisión específicamente no se denomina el cargo como Oficial de Protección de Datos Personales, el que es de implementación voluntaria conforme lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Sinaloa; en virtud de que en el Reglamento Interior de este organismo garante se eleva la figura a nivel de Dirección, siendo la Dirección de Datos Personales la encargada de proponer las políticas, parámetros, criterios y demás acciones para el cumplimiento de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Sinaloa y demás normativa aplicable en la materia; con las facultades y atribuciones de ley, conforme lo mandata el artículo 52 del Reglamento Interior de esta Comisión y que a la letra establece:

> ***"Artículo 52.*** *Corresponde a la Dirección de Datos Personales el ejercicio y cumplimiento de las siguientes facultades y obligaciones:*
>
> ***I.*** *Plantear al Pleno la interpretación de la Ley de Protección de Datos y normatividad aplicable en la materia, cuando así se le solicite;*
>
> ***II.*** *Proponer al Pleno las políticas, parámetros, criterios y demás disposiciones de las diversas materias a que se refiere la Ley de Protección de Datos, así como las modificaciones que resulten aplicables, para impulsar el derecho a la protección de los datos personales y con ello su tutela, tratamiento, seguridad y protección de aquéllos que se encuentren en posesión de los sujetos obligados;*

*III.* *Adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en posesión de la Comisión, a fin de que no se altere la veracidad de éstos;*

*IV.* *Proponer al Pleno para su aprobación los Avisos de Privacidad de esta Comisión y mantenerlos vigentes en el portal Institucional;*

*V.* *Establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad;*

*VI.* *Elaborar y someter a la aprobación del Pleno un documento que contenga las medidas de seguridad de carácter físico, técnico y administrativo conforme a lo dispuesto en la Ley de Protección de Datos y demás disposiciones que resulten aplicables en la materia;*

*VII.* *Llevar una bitácora de las vulneraciones a la seguridad;*

*VIII.* *Establecer controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales, guarden confidencialidad respecto de éstos, obligación que subsistirá aún después de finalizar sus relaciones con el mismo;*

*IX.* *Elaborar los formatos de solicitudes para el ejercicio de los derechos ARCO, así como establecer mecanismos adicionales, tales como, formularios, sistemas y otros medios simplificados para facilitar a los titulares su ejercicio;*

*X.* *Desarrollar o adoptar, en lo individual o en acuerdo con otros responsables, encargados u organizaciones, esquemas de mejores prácticas en materia de protección de datos personales;*

*XI.* *Elaborar un programa de capacitación y actualización al personal de la Comisión sobre las obligaciones y demás deberes en materia de protección de datos personales;*

*XII.* *Capacitar y actualizar de forma permanente a los servidores públicos de los sujetos obligados en materia de protección de datos personales, a través de la impartición de cursos, seminarios, talleres y cualquier otra forma de enseñanza y entrenamiento que se considere pertinente;*

*XIII.* *Proporcionar a los Comisionados el apoyo técnico necesario durante la sustanciación de los procedimientos previstos en la Ley de Protección de Datos y demás normatividad aplicable en la materia;*

*XIV.* *Llevar a cabo las auditorías a las que voluntariamente se sometan los sujetos obligados y que tengan por objeto verificar la adaptación, adecuación y eficacia*

*de los controles, medidas y mecanismos implementados para el cumplimiento de las disposiciones previstas en la ley de Protección de Datos y demás normativa que resulte aplicable; y*

***XV.*** *Las demás que señalen el Pleno, el Comisionado o Comisionada Presidente, la Ley General de Protección de Datos, la Ley de Protección de Datos, este Reglamento y las demás disposiciones que resulten aplicables en la materia."*

Se anexa a la presente respuesta copia escaneada de la suscrita, como Directora de Datos Personales.

***18. "Cuántas transferencias han realizado en materia de datos personales en este año 2024."***

En respuesta a la pregunta que se contesta, se hace de su conocimiento que, no se generan estadísticas respecto al número de transferencias realizadas en materia de datos personales.

Asimismo, se informa que, conforme al documento de seguridad de este organismo garante, la única área administrativa facultada para realizar transferencias de datos personales, de acuerdo a la finalidad con la que son recabados los mismos, es la Dirección de Administración.

Es importante señalar que, el resto de áreas responsables precisadas en el documento de seguridad, no realizará ninguna transferencia de datos personales, salvo aquéllas que sean necesarias para atender requerimientos de información de una autoridad competente, que estén debidamente fundados y motivados y actualicen alguno de los supuestos previstos por el artículo 89 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Sinaloa, para cuyo caso no será necesario recabar el consentimiento del titular.

En lo concerniente a esta Dirección de Datos Personales, se informa que no realiza tratamiento de datos personales de titulares, por lo que, durante este año de 2024, se han realizado 0 (cero) transferencias de datos personales a terceros.

***19. "Cuentan con el Programa Integral de Gestión de Datos, en caso de contar con dicho programa se me proporcione".***

En respuesta a la pregunta que se contesta, se hace de su conocimiento que, la normativa mexicana en materia de datos personales no contempla textualmente un Programa Integral de Gestión de Datos Personales como el señalado por la parte

solicitante, por lo que, no se cuenta con el programa en mención, ni existe obligación de contar con éste.

No obstante, en un ejercicio de dar una interpretación amplia al objeto de la solicitud, se informa que 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:

- Guía de información confidencial.
- Lineamientos internos para el uso de videovigilancia en las instalaciones de la CEAIP.
- Protocolo para la Protección de Datos Personales en Documentos Físicos, Electrónicos y Digitales al interior de la CEAIP.
- Protocolo ante vulneraciones de datos personales.
- Programa General de Capacitación.
- Inventario de datos personales y sistemas de tratamiento.

***20. "Qué mecanismos han implementado y/o realizado para asegurar que los datos personales se entregue solo a sus titulares y/o representantes."***

En relación a la pregunta que se contesta, se hace de su conocimiento que, se realizan diversas capacitaciones en materia de datos personales, por parte de esta Dirección, a fin de que el personal de la Comisión cuente con los conocimientos necesarios para detectar aquella información que es de carácter confidencial, y en su caso, solicitar la clasificación de la información correspondiente al Comité de Transparencia y generar versiones públicas conforme la ley en la materia, con el propósito de evitar que datos personales sean entregados a personas diversas de sus titulares o representantes y se vulneren por consiguiente datos personales.

Además de lo anterior, se han elaborado diversos documentos que contribuyen a la protección en el tratamiento de datos personales como lo son:

- Guía de Información Confidencial de la Dirección de Administración de la CEAIP.
- Lineamientos Internos para el uso de videovigilancia en las instalaciones de la Comisión Estatal para el Acceso a la Información Pública.
- Protocolo para la Protección de datos personales en documentos físicos, electrónicos y digitales al interior de la CEAIP.
- Bitácora de Vulneraciones.
- Formato de Registro de Salida de Soportes Físicos.
- Lineamientos para la recepción de documentos del personal de la CEAIP y llenado de la Ficha curricular.
- Compromiso de confidencialidad.

***21. "Cuántas auditorías en materia de datos personales han realizado a los sujetos obligados desde el 2010 a la fecha y cuáles son esos sujetos obligados."***

En relación a la pregunta que se contesta, se hace de su conocimiento que, de conformidad con lo establecido en el artículo 52, fracción XIV, esta Dirección de Datos Personales, es competente para llevar a cabo únicamente las auditorías a las que voluntariamente se sometan los sujetos obligados y que tengan por objeto verificar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados para el cumplimiento de las disposiciones previstas en la ley de Protección de Datos y demás normativa que resulte aplicable.

En razón de lo anterior, se informa que, del año 2010 a la fecha no se han requerido auditorias voluntarias parte por parte de los Sujetos Obligados, por lo que, el número de auditorías voluntarias realizadas en materia de datos personales a sujetos obligados es de 0 (cero).

***22. "Se me explique cuáles son las medidas que aplican para uno de los principios incorporados en la LGPDPPSO, para garantizar el tratamiento de los datos personales."***

En relación a la pregunta que se contesta, se hace de su conocimiento que, uno de los principios contemplados en la Ley General de Protección de Datos Personales en Posesión de Subjetos Obligados y su correlativo en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligado del Estado de Sinaloa, es el **principio de calidad**, que consiste en la exactitud y veracidad de los datos personales tratados, es decir, el deber del sujeto obligado en mantener completos, correctos y actualizados dichos datos.

De acuerdo a lo anterior, esta comisión ha implementado diversas medidas de seguridad como las siguientes:

**a) Medidas de Seguridad Administrativas.**

- Guía de información confidencial.
- Lineamientos internos para el uso de videovigilancia en las instalaciones de la CEAIP.
- Protocolo para la Protección de Datos Personales en Documentos Físicos, Electrónicos y Digitales al interior de la CEAIP.
- Protocolo ante vulneraciones de datos personales.
- Programa General de Capacitación.
- Inventario de datos personales y sistemas de tratamiento.

**b) Medidas de Seguridad Físicas.**

- Acceso regulado mediante credenciales electrónicas personales
- Oficinas privadas
- Gavetas o archiveros.
- Señalización de acceso restringido
- Detector de humo.
- Extintores.
- Cámaras de seguridad.
- Registro de salida de equipos de cómputo y/o dispositivos electrónicos.

**c) Medidas de Seguridad Técnicas.**

- Usuario y contraseñas.
- Antivirus.
- Copias de seguridad o respaldos de la información.
- Formas de supresión y borrado seguro de información (electrónica).
- Mantenimiento de equipo.
- Instalación y uso de software controlado.
- Firewall y DMZ
- Tickets para atención de información en la Plataforma Nacional de Transparencia

***23. "Qué sujetos obligados han presentado su evaluación de impacto en la protección de datos personales en los años 2020 a la fecha."***

En relación a la pregunta que se contesta, se hace de su conocimiento que, durante el año 2020 a la fecha no se han presentado evaluaciones de impacto por parte de los Sujetos Obligados ante este organismo garante, por lo tanto, el número de sujetos obligados que han presentado su evaluación de impacto en la protección de datos personales en el periodo señalado, es igual a 0 (cero).

***24. "Cuantas recomendaciones no vinculantes han emitido sobre el contenido de la evaluación de impacto de los años 2020 a la fecha."***

En relación a la pregunta que se contesta, se hace de su conocimiento que, toda vez que, durante el año 2020 a la fecha no se han presentado evaluaciones de impacto por parte de los Sujetos Obligados ante este organismo garante, el número de recomendaciones no vinculantes emitidas sobre el contenido de la evaluación de impacto de los años 2020 a la fecha es igual a 0 (cero).

En ese tenor, en relación a la pregunta que se responde y a todas las demás en las que se ha señalado como respuesta 0 (cero), es importante precisar que la respuesta en el sentido cero se entiende como un dato que constituye un elemento numérico que atiende a la solicitud y no debe entenderse como la inexistencia de la información solicitada, por lo que no se considera necesario que esta declaración sea sometida ante el Comité de Transparencia.

Como sustento de lo anterior, se cita el Criterio orientador con Clave de Control SO/018/2013 emitido por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)[1], que a letra dice:

> ***Respuesta igual a cero. No es necesario declarar formalmente la inexistencia.*** *En los casos en que se requiere un dato estadístico o numérico, y el resultado de la búsqueda de la información sea cero, éste deberá entenderse como un dato que constituye un elemento numérico que atiende la solicitud, y no como la inexistencia de la información solicitada. Por lo anterior, en términos del artículo 42 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, el número cero es una respuesta válida cuando se solicita información cuantitativa, en virtud de que se trata de un valor en sí mismo.*

Sin más por el momento, reciba un cordial saludo.

Atentamente

**Lic. Teresita Castro Aguilasocho**
Directora de Datos Personales

---

[1] **Precedentes:**

- Acceso a la información pública. 4301/11. Sesión del 11 de octubre de 2011. Votación por unanimidad. Sin votos disidentes o particulares. Secretaría de Comunicaciones y Transportes. Comisionada Ponente Sigrid Arzt Colunga.
- Acceso a la información pública. RDA 2111/12. Sesión del 11 de julio de 2012. Votación por unanimidad. Sin votos disidentes o particulares. Presidencia de la República. Comisionada Ponente María Elena Pérez-Jaén Zermeño.
- Acceso a la información pública. RDA 4451/12. Sesión del 23 de enero de 2013. Votación por unanimidad. Sin votos disidentes o particulares. Procuraduría Federal de la Defensa del Trabajo. Comisionada Ponente María Elena Pérez-Jaén Zermeño.
- Acceso a la información pública. RDA 0455/13. Sesión del 17 de abril de 2013. Votación por unanimidad. Sin votos disidentes o particulares. Instituto Nacional de Migración. Comisionado Ponente Ángel Trinidad Zaldívar.
- Acceso a la información pública. RDA 2238/13. Sesión del 19 de junio de 2013. Votación por unanimidad. Sin votos disidentes o particulares. Procuraduría General de la República. Comisionada Ponente María Elena Pérez-Jaén Zermeño.