

“2024, Año de Felipe Carrillo Puerto, Benemérito del Proletariado, Revolucionario y Defensor del Mayab”

**ACUERDO DE RESPUESTA
UNIDAD DE TRANSPARENCIA
SOLICITUD DE ACCESO A LA INFORMACIÓN
NÚMERO DE FOLIO 070116524000021**

CENTRO ESTATAL DE PREVENCIÓN SOCIAL DE LA VIOLENCIA Y PARTICIPACIÓN CIUDADANA (CEPSVYPC).- UNIDAD DE TRANSPARENCIA.- TUXTLA GUTIÉRREZ, CHIAPAS; A MIÉRCOLES 02 DOS DE OCTUBRE DE 2024 DE DOS MIL VEINTICUATRO.

Con fecha 17 diecisiete de septiembre de 2024 dos mil veinticuatro se tuvo por presentada la Solicitud de Información con número de folio 070116524000021, a través de la Plataforma Nacional de Transparencia (PNT) por el/la solicitante **Griselda Tobias Angulo**. En la solicitud anteriormente señalada, se realiza el requerimiento de la siguiente información a través de documentación anexa:

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.?

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.

Solicito su programa de capacitación en materia de datos personales han aplicado en su institución y/o dependencia de los años 2023 y 2024.

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

“2024, Año de Felipe Carrillo Puerto, Benemérito del Proletariado, Revolucionario y Defensor del Mayab”

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.

Cuántas solicitudes de derechos ARCOP han recibido desde de los años 2010 a la fecha, además se informe por mes cuántas han recibido y esas cuantas ha sido de acceso, rectificación, cancelación, oposición y de portabilidad, y cuántas son hombres y mujeres y cuales se han declarado la inexistencia de los datos personales.

Copia escaneada del nombramiento de su oficial de protección de datos personales. Solicito el programa de capacitación del comité de transparencia y/o unidad de transparencia y/o oficial de protección de datos personales en materia de protección de datos personales de los años 2023 y 2024.

Se me informe sobre los procedimientos que han implementado y/o realizado para la eficiencia de la gestión de las solicitudes de derechos ARCOP y que área lo realizó.

Cuántas transferencias han realizado en materia de datos personales en este año 2024 y que áreas administrativas lo han realizado 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.

Cuántos servidores públicos integran su unidad de transparencia. Cuántas auditorías en materia de datos personales le han solicitado al órgano garante desde el 2010 a la fecha.

Se me informe si han remitido el informe semestral referente al número de requerimientos de localización geográfica en tiempo real y de registro de datos realizados, así como el número de registros de datos de comunicaciones cancelados y suprimidos de manera segura, una vez cumplido el fin para el cual fueron solicitados, de los años 2010 a la fecha.

Referente al informe antes solicitado se me entregue el link donde pueda consultar la información estadística de dicho informe.

Cuántas denuncias en materia de datos personales han recibido desde el años 2010 a la fecha 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.

Cuántas recomendaciones no vinculantes han emitido sobre el contenido de la evaluación de impacto de los años 2020 a la fecha.

Cuántas denuncias en materia de obligaciones de transparencia han recibido desde el año 2020 a la fecha y el sentido de la resolución.

“2024, Año de Felipe Carrillo Puerto, Benemérito del Proletariado, Revolucionario y Defensor del Mayab”

Qué programa y/o acciones han implementado en materia de gobierno abierto.

Al respecto y con fundamento en el artículo 70, fracción II, IV, V así como del artículo 148 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas, considerando que esta Unidad de Transparencia es competente para recibir y dar trámite a las solicitudes de acceso a la información y de datos personales dirigidas al Centro Estatal de Prevención Social de la Violencia y Participación Ciudadana, así como de notificar a los solicitantes las resoluciones, realizó las gestiones correspondientes solicitando mediante memorándum la información a la Responsable de Datos Personales, de acuerdo a la normatividad aplicable y con ello estar en condiciones de dar respuesta a la petición en comento.

La Responsable de Datos Personales remitió a esta Unidad de Transparencia un memorándum con la siguiente información:

1.- Se me informe ¿qué políticas en materia de protección de datos personales han diseñado y/o Implementado? **Algunas políticas en materia de protección de datos personales las encontrará en el Documento de Seguridad ubicado en nuestra página oficial www.prevencion.chiapas.gob.mx, de lo anterior me permito anexar dicho documento a la solicitud con Folio No. 070116524000021 y señalar lo siguiente:**

Las medidas generales de seguridad administrativas, físicas y técnicas con las que actualmente cuenta el CEPsVyPC para mantener la confidencialidad e integridad de la información, para proteger los datos personales contra daño, pérdida, destrucción o alteración, así como evitar el uso, acceso o tratamiento no autorizado, e impedir la divulgación no autorizada, son las siguientes:

A) Medidas administrativas

- 1. Diseño y desarrollo de un modelo de capacitación permanente en materia de la Ley de Protección de Datos Personales en posesión de Sujetos Obligados del Estado de Chiapas (LPDPPSOCHIS), impartido a quienes colaboran en el CEPsVyPC.**
- 2. Implementación de formatos de entrada y salida de préstamo de documentos por parte del área encargada del archivo.**
- 3. Resguardo de los expedientes bajo los criterios, directrices y lineamientos para la atención de los expedientes técnicos.**
- 4. Mecanismos de control desarrollados conforme a lo establecido en los lineamientos del Sistema de Gestión de Documentos Institucional.**
- 5. Suscripción de una carta responsiva por parte de los usuarios o personal con acceso a sistemas de datos personales, acerca del deber de confidencialidad.**
- 6. Reportar al superior jerárquico los incidentes detectados respecto de pérdida o alteración de cualquier documento que contengan datos personales.**

B) Medidas físicas

- 1. Resguardo de documentos e información en archivos físicos de trámite y concentración.**
- 2. Disponer de la instalación de chapas con llave para mantener control de acceso de personas a espacios de resguardo de información.**

“2024, Año de Felipe Carrillo Puerto, Benemérito del Proletariado, Revolucionario y Defensor del Mayab”

3. Limitar el número de personas con acceso a archivos físicos.
4. Realizar el registro de personas con acceso a espacios físicos en los que se resguarda información con datos personales.
5. Procurar suscribir responsivas de confidencialidad con el personal que trata datos personales.
6. Designación de personal con acceso controlado a espacios de resguardo físico de expedientes y documentos con datos personales.
7. Resguardo de llaves en oficinas de acceso restringido.

C) Medidas técnicas

1. Utilizar claves de usuario y contraseñas de manera personal, y evitar compartirlas, prestarlas o registrarlas a la vista de otras personas.
2. Establecer y utilizar contraseñas robustas, es decir, de al menos ocho caracteres alfanuméricos y especiales, evitando que sean iguales al nombre del usuario, o cualquier otro nombre de personas, considerando que éstas sean fáciles de recordar y difíciles de adivinar o descifrar por un tercero, a fin de salvaguardar la información y datos personales a los que se tenga acceso.
3. Notificar de manera inmediata al Área de Apoyo Administrativo los casos en los que los usuarios identifiquen o consideren que sus claves de usuario y/o contraseñas han sido utilizadas por un tercero, para las prevenciones conducentes.
4. Procurar la utilización de una cuenta de correo electrónico oficial para fines relacionados con las actividades laborales, evitando remitir datos personales.
5. Mantener los documentos electrónicos y físicos en lugares seguros, bajo llave, dentro de cajones cerrados, o bajo la protección de alguna contraseña, a fin de promover la restricción a los datos personales que pudieran contener.
6. No difundir, transmitir o compartir documentos electrónicos ni físicos que contengan datos personales, a fin de garantizar que estos no sean divulgados de manera no autorizada.
7. Evitar dejar u olvidar los documentos físicos que contengan datos personales en los equipos de impresión, así como evitar su impresión, escaneo y fotocopiado si no es realmente requerido para las actividades laborales.
8. Evitar el acceso a los sistemas de información de tratamiento de datos personales, bajo el precepto del mínimo privilegio; es decir, únicamente al personal que por sus funciones y facultades laborales los requiera, a fin de mantener una adecuada segregación de funciones, restricción de acceso y tratamiento de esos datos.
9. Borrar o eliminar de la papelería de reciclaje del escritorio de los equipos de cómputo los documentos o archivos electrónicos que nos son necesarios para el desarrollo de funciones.
10. Notificar las bajas de accesos a los sistemas de información o de tratamiento de datos personales, con oportunidad, para restringir el acceso a dichos datos por personal no autorizado.

2.- Se me entregue el documento de seguridad. **Se anexa Documento de Seguridad Actualizado a esta solicitud con Folio No. 070116524000021, además podrá encontrarlo en nuestra página oficial www.prevencion.chiapas.gob.mx .**

3.- ¿Qué medidas de seguridad han adoptado para mantener exactos, completos, correcto y

“2024, Año de Felipe Carrillo Puerto, Benemérito del Proletariado, Revolucionario y Defensor del Mayab”

actualizados los datos personales? No se ha realizado actualización de datos personales, en consideración que el Titular de estos lo solicite, de lo anterior me permito señalar lo siguiente: De acuerdo con el artículo 50 de la LPDPPSOCHIS, el análisis de riesgo y de brecha forma parte del documento de seguridad, como un medio para identificar las medidas de seguridad implementadas y, en relación con ello, las amenazas de vulneración en que se encuentran los datos personales. El análisis sirve para identificar el riesgo inherente a los datos personales en el tratamiento a que son sometidos en el ejercicio de las funciones del Centro Estatal de Prevención Social de la Violencia y Participación Ciudadana, con respeto a la integridad de las personas.

La evaluación de riesgos de los datos personales forma parte de la serie de elementos que integran el documento de seguridad, cuyo propósito es garantizar la confidencialidad, integridad y disponibilidad de los datos personales en posesión del CEPVPC. Asimismo, para el análisis de riesgo se han tomado en cuenta lo establecido en el lineamiento para la protección de datos personales del estado de Chiapas, que en su artículo 55, define que para el cumplimiento al artículo 47 fracción IV de la Ley Estatal, el responsable deberá realizar un análisis de riesgo de los datos personales tratados considerando lo siguiente:

- I. Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico;
- II. El valor de los datos personales de acuerdo con su clasificación previamente definitiva y su ciclo de vida;
- III. El valor y exposición de los activos involucrados en el tratamiento de los datos personales;
- IV. Las consecuencias y negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida; y
- V. Los factores previstos en el artículo 47 de la Ley Estatal.

Bajo esta premisa, para analizar los riesgos de los datos personales que son objeto de tratamiento por el CEPVPC, se aplicó un instrumento para, primeramente, clasificar los datos utilizados, a partir de la categorización existente en la ley:

- 1) De identificación o contacto, que se refieren a información por la que se identifica a una persona y/o permiten su contacto como, por ejemplo, el nombre, el domicilio, el correo electrónico, la firma, los usuarios, el Registro Federal de Contribuyentes, la Clave Única de Registro de Población o la edad.
- 2) Patrimoniales, que comprenden la información que se encuentran vinculados al patrimonio de una persona como, por ejemplo, el salario, los créditos, las tarjetas de débito, los cheques o las inversiones.
- 3) Sensibles, que consideran la información concerniente a la esfera más íntima de su titular o que su uso puede dar origen a discriminación o conlleva un riesgo grave para éste como, por ejemplo, el origen étnico, el estado de salud presente o futuro, las creencias religiosas, la opinión política o la orientación sexual.

De los anteriores, se identificó que se trabaja sobre todo con dos categorías: datos de identificación y datos patrimoniales, ya que como datos sensibles solamente se recuperan datos de salud.

En un segundo momento, para la determinación del riesgo sobre esa tipología de datos personales se valoró la probabilidad e impacto de que, en su obtención, almacenamiento, tratamiento,

“2024, Año de Felipe Carrillo Puerto, Benemérito del Proletariado, Revolucionario y Defensor del Mayab”

transferencia o remisión, bloqueo y/o eliminación (ciclo de vida), en correspondencia con la cantidad de datos involucrados, se materialice uno o más factores que pueden causar un daño a su titular (amenaza).

4.- ¿Qué procedimientos han establecidos para la conservación y en su caso, bloqueo y supresión de los datos personales? **Las técnicas utilizadas para la conservación y supresión segura de los datos personales, es un tema de vital importancia para proteger la privacidad, confidencialidad, integridad y disponibilidad de la información, y en particular de los datos personales; debe hacerse bajo procedimientos que garanticen que fueron eliminados en su totalidad y que no pueden ser recuperados, y utilizarse de manera indebida, por lo que me permito hacer de conocimiento que el Centro Estatal de Prevención Social de la Violencia y Participación Ciudadana se guía por el Sistema Institucional de Archivo (SIA) y los Lineamientos para la Organización y Conservación de Archivos en el Estado de Chiapas que expresa lo siguiente: El Sistema Institucional de Archivos (SIA) es definido en la Ley General de Archivos (LGA) como: “El conjunto de registros, procesos, procedimientos, criterios, estructuras, herramientas y funciones que desarrolla cada sujeto obligado y sustenta la actividad archivística, de acuerdo con los procesos de gestión documental”. Todos los documentos de archivo en posesión de los sujetos obligados formarán parte del sistema institucional; deberán agruparse en expedientes de manera lógica y cronológica, y relacionarse con un mismo asunto, reflejando con exactitud la información contenida en ellos, en los términos que establezca el Consejo Nacional de Archivos y las disposiciones jurídicas aplicables.**

¿Qué es el ciclo vital del documento?

El ciclo vital del documento es la denominación que se le da a las distintas fases o etapas que pasa el documento, desde su creación hasta su eliminación o selección para su custodia permanente y se establece en función de los valores de los documentos y frecuencia de uso.

Las fases o etapas que conforman el ciclo vital del documento son:

Archivo de trámite: es aquel donde se reúne la documentación que se encuentra en gestión, en busca de solución a los asuntos iniciados, la cual es sometida a continua utilización y consulta administrativa por las mismas oficinas u otras que lo soliciten.

Archivo de concentración: es aquel donde se agrupan los documentos transferidos por las áreas administrativas, una vez que se finalizó su trámite, pero siguen siendo vigentes con objeto de consulta por las propias áreas.

Archivo histórico: es aquel donde se resguarda la documentación que transfiere el archivo de concentración, sólo los documentos con valor permanente.

Es importante señalar que la LGA establece que las instituciones deben tener un sistema institucional para la administración de sus archivos. Las mismas instituciones son las responsables de la organización, conservación y buen funcionamiento de su sistema institucional de archivos.

¿Quiénes lo integran?

De conformidad con lo establecido en el artículo 21 de la Ley General de Archivos (LGA), el Sistema Institucional de cada sujeto obligado deberá integrarse por:

Un área coordinadora de archivos, y Las áreas operativas siguientes:

De correspondencia; Archivo de trámite, por área o unidad; Archivo de concentración, y Archivo

“2024, Año de Felipe Carrillo Puerto, Benemérito del Proletariado, Revolucionario y Defensor del Mayab”

histórico, en su caso, sujeto a la capacidad presupuestal y técnica del sujeto obligado.

5.- ¿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? **Derechos ARCOP el cual consiste en lo siguiente:**

Derechos ARCOP

Los titulares (dueños) de los datos personales, tienen el derecho de acceder a ellos, rectificarlos, a solicitar que se eliminen o cancelen, a oponerse a su uso, así como a la portabilidad sobre el tratamiento de estos, ante el sujeto obligado o responsable que este en posesión de los mismos.

A continuación se explica en qué consiste cada uno de estos derechos:

Derecho de Acceso a Datos Personales

Es aquel que consiste en solicitar el acceso a los datos personales que están en las bases de datos, sistemas, archivos, registros o expedientes del responsable que los posee, almacena o utiliza, así como de conocer información relacionada con el uso que se da a la información personal.

Derecho de Rectificación de Datos Personales

Es el derecho de solicitar la rectificación o corrección de datos personales, cuando éstos sean inexactos o incompletos o no se encuentren actualizados. Es decir se puede solicitar a quien posea o utilice los datos personales que los corrija cuando los mismos sean incorrectos, desactualizados o inexactos.

Derecho de Cancelación de Datos Personales

Consistente en solicitar que los datos personales se eliminen de los archivos, registros, expedientes, sistemas, bases de datos del responsable que los posee, almacena o utiliza. Aunque hay que tomar en cuenta que no en todos los casos se podrán eliminar los datos personales, principalmente cuando sean necesarios por alguna cuestión legal o para el cumplimiento de obligaciones.

Derecho a la Oposición de Datos Personales

Es el derecho que se tiene de solicitar que los datos personales no se utilicen para ciertos fines, o de requerir que se concluya el uso de los mismos a fin de evitar un daño al titular de estos datos. Al igual en este caso, como en el anterior, no siempre se podrá impedir el uso de los datos personales, cuando sean necesarios por alguna cuestión legal o para el cumplimiento de obligaciones.

Portabilidad de Datos Personales

Es el derecho de obtener del responsable que posee los datos personales, una copia de la información que obre en sus archivos.

El titular tendrá el derecho a obtener del responsable una copia de los datos personales objeto del tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos.

“2024, Año de Felipe Carrillo Puerto, Benemérito del Proletariado, Revolucionario y Defensor del Mayab”

Avisos de Privacidad Integrales y Simplificados, mismos que se encuentran en nuestra página oficial www.prevencion.chiapas.gob.mx y que hablan acerca de este tipo de derechos (ARCO).

6.- ¿Qué mecanismos han utilizados y/o aplicados para cumplir con los plazos fijados para la supresión de los datos personales? **Las técnicas utilizadas para la supresión segura de los datos personales, es un tema de vital importancia para proteger la privacidad, confidencialidad, integridad y disponibilidad de la información, y en particular de los datos personales; debe hacerse bajo procedimientos que garanticen que fueron eliminados en su totalidad y que no pueden ser recuperados, y utilizarse de manera indebida, por lo que me permito hacer de conocimiento que el Centro Estatal de Prevención Social de la Violencia y Participación Ciudadana se guía por el Sistema Institucional de Archivo (SIA) y los Lineamientos para la Organización y Conservación de Archivos en el Estado de Chiapas que expresa lo siguiente: El Sistema Institucional de Archivos (SIA) es definido en la Ley General de Archivos (LGA) como: “El conjunto de registros, procesos, procedimientos, criterios, estructuras, herramientas y funciones que desarrolla cada sujeto obligado y sustenta la actividad archivística, de acuerdo con los procesos de gestión documental”. Todos los documentos de archivo en posesión de los sujetos obligados formarán parte del sistema institucional; deberán agruparse en expedientes de manera lógica y cronológica, y relacionarse con un mismo asunto, reflejando con exactitud la información contenida en ellos, en los términos que establezca el Consejo Nacional de Archivos y las disposiciones jurídicas aplicables.**

¿Qué es el ciclo vital del documento?

El ciclo vital del documento es la denominación que se le da a las distintas fases o etapas que pasa el documento, desde su creación hasta su eliminación o selección para su custodia permanente y se establece en función de los valores de los documentos y frecuencia de uso.

Las fases o etapas que conforman el ciclo vital del documento son:

Archivo de trámite: es aquel donde se reúne la documentación que se encuentra en gestión, en busca de solución a los asuntos iniciados, la cual es sometida a continua utilización y consulta administrativa por las mismas oficinas u otras que lo soliciten.

Archivo de concentración: es aquel donde se agrupan los documentos transferidos por las áreas administrativas, una vez que se finalizó su trámite, pero siguen siendo vigentes con objeto de consulta por las propias áreas.

Archivo histórico: es aquel donde se resguarda la documentación que transfiere el archivo de concentración, sólo los documentos con valor permanente.

Es importante señalar que la LGA establece que las instituciones deben tener un sistema institucional para la administración de sus archivos. Las mismas instituciones son las responsables de la organización, conservación y buen funcionamiento de su sistema institucional de archivos.

¿Quiénes lo integran?

De conformidad con lo establecido en el artículo 21 de la Ley General de Archivos (LGA), el Sistema Institucional de cada sujeto obligado deberá integrarse por:

“2024, Año de Felipe Carrillo Puerto, Benemérito del Proletariado, Revolucionario y Defensor del Mayab”

Un área coordinadora de archivos, y Las áreas operativas siguientes:

De correspondencia; Archivo de trámite, por área o unidad; Archivo de concentración, y Archivo histórico, en su caso, sujeto a la capacidad presupuestal y técnica del sujeto obligado.

De conformidad con lo dispuesto por el artículo 11 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Ley), uno de los principios que regula el derecho a la protección de datos personales es el de “calidad”. Este principio señala, entre otras cuestiones, que cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, es decir, borrados, suprimidos, eliminados o destruidos.

En el mismo sentido, el artículo 37 del Reglamento de la Ley establece que una vez cumplidas las finalidades del tratamiento, y cuando no exista disposición legal o reglamentaria que establezca lo contrario, el responsable deberá proceder a la cancelación de los datos personales en su posesión, previo bloqueo de los mismos, para su posterior supresión.

Es decir, el principio de calidad establece que, conforme a la finalidad o finalidades para las que se vayan a tratar los datos personales, éstos deben ser exactos, completos, pertinentes, actualizados y correctos. Asimismo, este principio señala que cuando los datos personales hayan dejado de ser necesarios para las finalidades para las cuales se obtuvieron, deben ser eliminados, tomando en cuenta las disposiciones legales aplicables para los plazos de conservación.

En ese sentido, con independencia de que un titular de los datos personales ejerza su derecho de cancelación, el responsable del tratamiento está obligado a eliminar, de oficio, los datos personales cuando hayan dejado de ser necesarios para la finalidad para la cual se obtuvieron.

El momento indicado para eliminar los datos personales depende del plazo de conservación de los mismos, el cual se fija a partir de las disposiciones legales aplicables en la materia de que se trate; los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información, y el periodo de bloqueo.

7.- En los años 2010 a la fecha ¿qué mecanismos y/o desarrollado han aplicado para la revisión periódica sobre la necesidad de conservar los datos personales y cuáles son? **El 22 de septiembre de 2022, inició el Diplomado del Sistema de Gestión de Datos Personales vía Zoom con personal del Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Chiapas, el 23 de enero del 2023, se emitió el dictamen favorable del Documento de Seguridad y el 9 de marzo del 2023, se emitió el dictamen favorable de los Avisos de Privacidad Integrales y Simplificado del CEPVPC, de lo anterior se solicitó al ITAIPCH la capacitación en materia de Datos Personales para el personal de este ente de Prevención mediante Oficio No. CEPVPC/DG/DP/337/2024 de fecha 28 de octubre de 2024, dando seguimiento a la propuesta de capacitación del Documento de Seguridad.**

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.? **No hay códigos de buenas prácticas, pero estamos respaldados con el monitoreo del Documento de Seguridad, el 22 de septiembre de 2022, inició el Diplomado del Sistema de Gestión de Datos Personales vía Zoom con personal del Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Chiapas, el**

“2024, Año de Felipe Carrillo Puerto, Benemérito del Proletariado, Revolucionario y Defensor del Mayab”

23 de enero del 2023 se emitió el dictamen favorable del Documento de Seguridad y el 9 de marzo del 2023, se emitió el dictamen favorable de los Avisos de Privacidad Integrales y Simplificado del CEPSVyPC, de lo anterior se solicitó al ITAIPCH la capacitación en materia de Datos Personales para el personal de este ente de Prevención mediante Oficio No. CEPSVyPC/DG/DP/337/2024 de fecha 28 de octubre de 2024, dando seguimiento a la propuesta de capacitación del Documento de Seguridad, dicho documento se encuentra en proceso de actualización.

9.- ¿Qué programas y/o políticas de protección de datos personales han implementado y/o realizado y/o elaborado ect.? El 22 de septiembre de 2022, inició el Diplomado del Sistema de Gestión de Datos Personales vía Zoom con personal del Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Chiapas, el 23 de enero del 2023, se emitió el dictamen favorable del Documento de Seguridad y el 9 de marzo del 2023, se emitió el dictamen favorable de los Avisos de Privacidad Integrales y Simplificado del CEPSVyPC, de lo anterior se solicitó al ITAIPCH la capacitación en materia de Datos Personales para el personal de este ente de Prevención mediante Oficio No. CEPSVyPC/DG/DP/337/2024 de fecha 28 de octubre de 2024, dando seguimiento a la propuesta de capacitación del Documento de Seguridad, dicho documento se encuentra en proceso de actualización.

10.- Solicito su programa de capacitación en materia de datos personales han aplicado en su institución y/o dependencia de los años 2023 y 2024. El 22 de septiembre de 2022, inició el Diplomado del Sistema de Gestión de Datos Personales vía Zoom con personal del Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Chiapas, el 23 de enero del 2023, se emitió el dictamen favorable del Documento de Seguridad y el 9 de marzo del 2023, se emitió el dictamen favorable de los Avisos de Privacidad Integrales y Simplificado del CEPSVyPC, de lo anterior se solicitó al ITAIPCH la capacitación en materia de Datos Personales para el personal de este ente de Prevención mediante Oficio No. CEPSVyPC/DG/DP/337/2024 de fecha 28 de octubre de 2024, dando seguimiento a la propuesta de capacitación del Documento de Seguridad.

11.- ¿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? Actualmente en nuestras redes sociales se encuentran las publicaciones de las infografías respecto a Datos Personales:

Facebook: Centro Estatal de Prevención Social de la Violencia Chiapas

<https://www.facebook.com/CEPSVyPCChiapas/>

X: Centro Estatal de Prevención Social Chiapas

<https://x.com/prevenchiapas>

De lo anterior anexo la evidencia de dichas publicaciones.

“2024, Año de Felipe Carrillo Puerto, Benemérito del Proletariado, Revolucionario y Defensor del Mayab”

12.- ¿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? El Documento de Seguridad y los Avisos de Privacidad Integrales y Simplificados del Centro Estatal se encuentran ubicados en nuestra página oficial www.prevencion.chiapas.gob.mx.

En las diferentes redes sociales encontrará las publicaciones de las infografías respecto a Datos Personales:

Facebook: Centro Estatal de Prevención Social de la Violencia Chiapas

<https://www.facebook.com/CEPSVyPCChiapas/>

X: Centro Estatal de Prevención Social Chiapas

<https://x.com/prevenchiapas>

De lo anterior anexo la evidencia de dichas publicaciones.

13.- ¿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? Algunas medidas de seguridad en materia de protección de datos personales las encontrará en el Documento de Seguridad ubicado en nuestra página oficial www.prevencion.chiapas.gob.mx, de lo anterior me permito anexar dicho documento a la solicitud con Folio No. 070116524000021 y señalar lo siguiente:

Las medidas generales de seguridad administrativas, físicas y técnicas con las que actualmente cuenta el CEPSVyPC para mantener la confidencialidad e integridad de la información, así como para proteger los datos personales contra daño, pérdida, destrucción o alteración, así como evitar el uso, acceso o tratamiento no autorizado, e impedir la divulgación no autorizada, son las siguientes:

A) Medidas administrativas

1. Diseño y desarrollo de un modelo de capacitación permanente en materia de la Ley de Protección de Datos Personales en posesión de Sujetos Obligados del Estado de Chiapas (LPDPPSOCHIS), impartido a quienes colaboran en el CEPSVyPC.

2. Implementación de formatos de entrada y salida de préstamo de documentos por parte del área encargada del archivo.

3. Resguardo de los expedientes bajo los criterios, directrices y lineamientos para la atención de los expedientes técnicos.

4. Mecanismos de control desarrollados conforme a lo establecido en los lineamientos del Sistema de Gestión de Documentos institucional.

5. Suscripción de una carta responsiva por parte de los usuarios o personal con acceso a sistemas de datos personales, acerca del deber de confidencialidad.

6. Reportar al superior jerárquico los incidentes detectados respecto de pérdida o alteración de cualquier documento que contengan datos personales.

B) Medidas físicas

1. Resguardo de documentos e información en archivos físicos de trámite y concentración.

2. Disponer de la instalación de chapas con llave para mantener control de acceso de personas a

“2024, Año de Felipe Carrillo Puerto, Benemérito del Proletariado, Revolucionario y Defensor del Mayab”

espacios de resguardo de información.

3. Limitar el número de personas con acceso a archivos físicos.

4. Realizar el registro de personas con acceso a espacios físicos en los que se resguarda información con datos personales.

5. Procurar suscribir responsivas de confidencialidad con el personal que trata datos personales.

6. Designación de personal con acceso controlado a espacios de resguardo físico de expedientes y documentos con datos personales.

7. Resguardo de llaves en oficinas de acceso restringido.

C) Medidas técnicas

1. Utilizar claves de usuario y contraseñas de manera personal, y evitar compartirlas, prestarlas o registrarlas a la vista de otras personas.

2. Establecer y utilizar contraseñas robustas, es decir, de al menos ocho caracteres alfanuméricos y especiales, evitando que sean iguales al nombre del usuario, o cualquier otro nombre de personas, considerando que éstas sean fáciles de recordar y difíciles de adivinar o descifrar por un tercero, a fin de salvaguardar la información y datos personales a los que se tenga acceso.

3. Notificar de manera inmediata al Área de Apoyo Administrativo los casos en los que los usuarios identifiquen o consideren que sus claves de usuario y/o contraseñas han sido utilizadas por un tercero, para las prevenciones conducentes.

4. Procurar la utilización de una cuenta de correo electrónico oficial para fines relacionados con las actividades laborales, evitando remitir datos personales.

5. Mantener los documentos electrónicos y físicos en lugares seguros, bajo llave, dentro de cajones cerrados, o bajo la protección de alguna contraseña, a fin de promover la restricción a los datos personales que pudieran contener.

6. No difundir, transmitir o compartir documentos electrónicos ni físicos que contengan datos personales, a fin de garantizar que estos no sean divulgados de manera no autorizada.

7. Evitar dejar u olvidar los documentos físicos que contengan datos personales en los equipos de impresión, así como evitar su impresión, escaneo y fotocopiado si no es realmente requerido para las actividades laborales.

8. Evitar el acceso a los sistemas de información de tratamiento de datos personales, bajo el precepto del mínimo privilegio; es decir, únicamente al personal que por sus funciones y facultades laborales los requiera, a fin de mantener una adecuada segregación de funciones, restricción de acceso y tratamiento de esos datos.

9. Borrar o eliminar de la papelería de reciclaje del escritorio de los equipos de cómputo los documentos o archivos electrónicos que no son necesarios para el desarrollo de funciones.

10. Notificar las bajas de accesos a los sistemas de información o de tratamiento de datos personales, con oportunidad, para restringir el acceso a dichos datos por personal no autorizado.

14.-Se me entregué en copia escaneada de la bitácora de las vulneraciones de seguridad que han tenido sobre los tratamientos de los datos personales. **No se ha empleado porque no ha habido vulneraciones, se anexa formato de bitácora de vulneraciones de seguridad de datos personales,**

“2024, Año de Felipe Carrillo Puerto, Benemérito del Proletariado, Revolucionario y Defensor del Mayab”

a la solicitud con Folio No. 070116524000021.

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

16.- ¿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? **Se anexa circular al personal de formato de carta compromiso de confidencialidad, no divulgación, reserva y resguardo de información y datos personales, a la solicitud con Folio No. 070116524000021.**

17.- ¿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? **44 servidores públicos, se anexa plantilla del personal de este Centro Estatal de Prevención, a la solicitud con Folio No. 070116524000021.**

18.- ¿Cuántas solicitudes de derechos ARCOP han recibido desde de los años 2010 a la fecha, además se informe por mes cuántas han recibido y esas cuantas ha sido de acceso, rectificación, cancelación, oposición y de portabilidad, y cuántas son hombres y mujeres y cuales se han declarado la inexistencia de los datos personales? **Ninguna.**

19.- Copia escaneada del nombramiento de su oficial de protección de datos personales. **Se anexa Nombramiento del Oficial de Datos Personales a esta solicitud con Folio No. 070116524000021, además podrá encontrarlo en nuestra página oficial www.prevencion.chiapas.gob.mx .**

20.- Solicito el programa de capacitación del comité de transparencia y/o unidad de transparencia y/o oficial de protección de datos personales en materia de protección de datos personales de los años 2023 y 2024. **El 22 de septiembre de 2022, inició el Diplomado del Sistema de Gestión de Datos Personales vía Zoom con personal del Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Chiapas, el 23 de enero del 2023, se emitió el dictamen favorable del Documento de Seguridad y el 9 de marzo del 2023, se emitió el dictamen favorable de los Avisos de Privacidad Integrales y Simplificado del CEPVPC, de lo anterior se solicitó al ITAIPCH la capacitación en materia de Datos Personales para el personal de este ente de Prevención mediante Oficio No. CEPVPC/DG/DP/337/2024 de fecha 28 de octubre de 2024, dando seguimiento a la propuesta de capacitación del Documento de Seguridad.**

21.- Se me informe sobre los procedimientos que han implementado y/o realizado para la eficiencia de la gestión de las solicitudes de derechos ARCOP y que área lo realizó. **No se han recibido solicitudes de Derechos ARCOP.**

“2024, Año de Felipe Carrillo Puerto, Benemérito del Proletariado, Revolucionario y Defensor del Mayab”

22.- ¿Cuántas transferencias han realizado en materia de datos personales en este año 2024 y que áreas administrativas lo han realizado?

Transferencias de Datos Personales Área de Apoyo Administrativo del CEPsVyPC	
Área	No. Transferencias
Recursos Humanos	88
Recursos Financieros	48
Planeación	0
Recursos Materiales	40
Jurídico	0
Informática	0
Total	176

23.- Cuentan con el Programa Integral de Gestión de Datos, en caso de contar con dicho programa se me proporcione. **Se anexan 2 Catálogos de Datos Personales a esta solicitud con Folio No. 070116524000021, 1 proporcionado en el Diplomado del Sistema de Gestión de Datos Personales vía Zoom con personal del Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Chiapas, mismos que se encuentran como parte de la información en el Documento de Seguridad que además podrá encontrarlo en nuestra página oficial www.prevencion.chiapas.gob.mx.**

24.- Qué mecanismos han implementado y/o realizado para asegurar que los datos personales se entregue solo a sus titulares y/o representantes. **Mediante la identificación y acreditación de la persona legal, señalado en la Ley Estatal de Protección de Datos Personales en Posesión de Sujetos Obligados.**

25.- Cuantos servidores públicos integran su unidad de transparencia. C. Perla Romina Piñón Sánchez, Responsable de la Unidad de Transparencia

26.- ¿Cuántas auditorías en materia de datos personales le han solicitado al órgano garante desde el 2010 a la fecha? **Ninguna, es importante remarcar que la Ley señala que dichas auditorías son a voluntad no a obligatoriedad.**

27.- Se me informe si han remitido el informe semestral referente al número de requerimientos de localización geográfica en tiempo real y de registro de datos realizados, así como el número de registros de datos de comunicaciones cancelados y suprimidos de manera segura, una vez cumplido

“2024, Año de Felipe Carrillo Puerto, Benemérito del Proletariado, Revolucionario y Defensor del Mayab”

el fin para el cual fueron solicitados, de los años 2010 a la fecha. **No se han suprimido datos personales aún, estamos en proceso de ello, debido a lo que nos marca la ley del Sistema Institucional de Archivos.**

28.- Referente al informe antes solicitado se me entregue el link donde pueda consultar la información estadística de dicho informe. **No aplica.**

29.- ¿Cuántas denuncias en materia de datos personales han recibido desde el años 2010 a la fecha? **Ninguna.**

30.- ¿Se me explique cuáles son las medidas que aplican para uno de los principios incorporados en la LGPDPSO, para garantizar el tratamiento de los datos personales? **De conformidad con lo establecido por el artículo 16 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPSO), los principios rectores en materia que todo responsable debe observar en el tratamiento de Datos PersonalesLos y los principios que rigen nuestro Documento de Seguridad son los siguientes:**

Licitud

El principio de Licitud, implica que todo tratamiento de datos personales por parte del responsable deberá sujetarse a las facultades o atribuciones que la normatividad aplicable le confiera.

Finalidad

El principio de Finalidad, implica que todo tratamiento de datos personales que efectué el responsable deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, en relación con las atribuciones expresas que la normatividad aplicable les confiera.

Lealtad

El principio de Lealtad, implica que el responsable no deberá obtener y tratar datos personales, a través de medios engañosos o fraudulentos, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad.

Calidad

El principio de calidad, implica que, el responsable deberá adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos y según se requiera para el cumplimiento de las finalidades concretas, explícitas lícitas y legítimas que motivaron su tratamiento.

Proporcionalidad

El principio de proporcionalidad, implica que el responsable sólo deberá tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad concreta, explícita lícita y legítima que justifica su tratamiento.

Información

“2024, Año de Felipe Carrillo Puerto, Benemérito del Proletariado, Revolucionario y Defensor del Mayab”

El principio de información, implica que el responsable deberá informar al titular a través del aviso de privacidad la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.

Responsabilidad

El principio de responsabilidad, se traduce en que el responsable deberá implementar los mecanismos previstos en el artículo 31 de la presente Ley para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en este ordenamiento; y rendir cuentas sobre el tratamiento de datos personales en su posesión al titular y al Instituto, debiendo observar para tal efecto la legislación aplicable en la materia. Así mismo, podrá valerse de estándares o mejores prácticas nacionales o internacionales para tales fines, en lo que no se contraponga con la normativa mexicana.

31.- ¿Qué sujetos obligados han presentado su evaluación de impacto en la protección de datos personales en los años 2020 a la fecha? **No aplica, cabe señalar que ese tipo de información no nos corresponde responderla, se debe solicitar al Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Chiapas, organismo que se encarga de realizar las evaluaciones de impacto.**

32.- ¿Cuántas recomendaciones no vinculantes han emitido sobre el contenido de la evaluación de impacto de los años 2020 a la fecha? **No aplica, cabe señalar que ese tipo de información no nos corresponde responderla, se debe solicitar al Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Chiapas, organismo que se encarga de realizar las evaluaciones de impacto.**

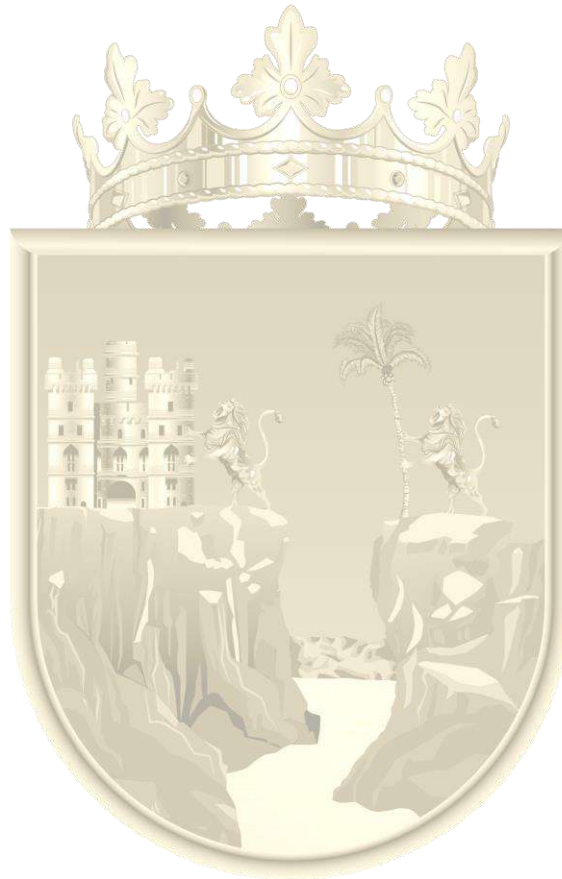
33.- ¿Cuántas denuncias en materia de obligaciones de transparencia han recibido desde el año 2020 a la fecha y el sentido de la resolución? En el siguiente link podrá encontrar la información solicitada <http://transparencia.chiapas.gob.mx/PortalGral/SolicitudesInformacion>

34.- ¿Qué programa y/o acciones han implementado en materia de gobierno abierto? Ninguno

Por lo anteriormente expuesto se tiene por atendida la presente solicitud de información, mediante el presente acuerdo y se le remite al Comité de Transparencia del CEPsVyPC para su notificación correspondiente.

Así lo notifica el servidor público Responsable de la Unidad de Transparencia del Centro Estatal de Prevención Social de la Violencia y Participación Ciudadana, quien actúa con fundamento en lo dispuesto en los artículos 67, 68, 70 fracción II, IV, V, 148, 149, 152 y 154 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS).-
RÚBRICA. -----

“2024, Año de Felipe Carrillo Puerto, Benemérito del Proletariado, Revolucionario y Defensor del Mayab”



CHIAPAS
GOBIERNO DEL ESTADO

Sujeto Obligado: Centro Estatal de Prevención Social de la Violencia y Participación Ciudadana.

Unidad Administrativa: Área o Dirección

Departamento: Unidad de Transparencia

Tratamiento o proceso: Solicitud de Acceso a la Información

Funcionarios que tratan datos personales (Nombre y Función)

CATÁLOGO DE DATOS PERSONALES

DATO PERSONAL SOLICITADO	SI	NO
Nombre de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros)		
Firma		
Antecedentes Laborales		
CURP		
RFC		
Año de nacimiento o edad		
Teléfono fijo o celular		
Correo electrónico		
Datos académicos		
Datos contenidos en declaraciones patrimoniales		
Datos de identificación		
Datos de salud		
País		
Estado		
Municipio		
Dirección		
Código Postal		
Número exterior y/o interior		
Razón Social		
Nombre del Representante Legal		
Primer Apellido del Representante Legal		
Segundo Apellido del Representante Legal		

GOBIERNO DEL ESTADO

Los datos personales recabados en este formato, serán protegidos, incorporados y tratados en los términos establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en los Lineamientos Generales para la Custodia y Protección de Datos Personales e Información Reservada y Confidencial en Posesión de los Sujetos Obligados del Estado de Chiapas y demás Normatividad aplicable.

La información de este documento, así como la contenida en los documentos que se adjuntan, puede ser objeto de solicitudes de acceso a la información pública, así mismo puede contener información confidencial o legalmente protegida y está destinado únicamente para el uso del destinatario (s) previsto. Cualquier divulgación, difusión, distribución, copia o la toma de cualquier acción basada en la información aquí contenida está prohibido.

Circular No. CEPsVyPC/DP/001/2024.
Tuxtla Gutiérrez, Chiapas.
04 de octubre del 2024.

SECCIÓN: 12C TRANSPARENCIA Y ACCESO DE INFORMACIÓN
SERIE: 12C.001. DISPOSICIÓN EN MATERIA DE ACCESO A LA INFORMACIÓN.

**A TODO EL PERSONAL DEL CENTRO ESTATAL DE PREVENCIÓN SOCIAL
DE LA VIOLENCIA Y PARTICIPACIÓN CIUDADANA.
PRESENTE.**

Por este medio, y con la finalidad de dar cumplimiento a lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, me permito hacerles llegar la Carta compromiso de confidencialidad, no divulgación, reserva y resguardo de información y datos personales, para su conocimiento y aplicación correspondiente.

Sin otro particular, les envío un cordial saludo.

ATENTAMENTE.


EDITH BECK CANO

OFICIAL DE PROTECCIÓN DE DATOS PERSONALES DEL CEPsVyPC.



ARCHIVO

La información de este memorándum, puede ser objeto de solicitudes de acceso a la información pública, así mismo puede contener información confidencial o legalmente protegida y está destinado únicamente para el uso del destinatario(s) previsto. Cualquier divulgación, distribución, copia o la toma de cualquier acción basada en la información aquí contenida está prohibida.

*Los datos personales recabados en este memorándum, serán protegidos, incorporados y tratados en los términos establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados Del Estado de Chiapas, así como en los Lineamientos Generales para la Custodia y Protección de Datos Personales e información Reservada y Confidencial en Posesión de los Sujetos Obligados del Estado de Chiapas y demás Normatividad.

CIRCULAR NO. CEPSVyPC/DP/001/2024

CARTA COMPROMISO DE CONFIDENCIALIDAD, NO DIVULGACIÓN, RESERVA Y RESGUARDO DE INFORMACIÓN Y DATOS PERSONALES.

Acepto la obligación de resguardo, reserva y protección de **confidencialidad** de la información, de datos personales y de todo tipo de documentos que reciba con motivo del desempeño de mi cargo. El presente compromiso me responsabiliza respecto de la información que me sea proporcionada con motivo del desempeño de mi cargo, ya sea escrita, impresa, electrónica, contenida en cualquier tipo de documento, sin importar su fuente o fecha de elaboración.

La información que me sea proporcionada podría ser considerada, según el caso, como reservada, privilegiada y confidencial, en los términos de las leyes aplicables, por lo que me obligo a protegerla, reservarla, resguardarla y no divulgarla, utilizándola única y exclusivamente para llevar a cabo y cumplir con las actividades y obligaciones que expresamente me sean asignadas por el Centro Estatal de Prevención Social de la Violencia y Participación Ciudadana.

Mi obligación de confidencialidad no es aplicable en los siguientes casos:

- A) Cuando la información sea del dominio público en el momento en que me sea suministrada o, una vez suministrada, ésta acceda al dominio público.
- B) Cuando la legislación vigente o un mandato judicial exija su divulgación.
- C) Cuando la legislación vigente o un mandato judicial exija su divulgación.

En el supuesto de que cese la relación laboral, por cualquier motivo, dicha obligación se extiende hasta un plazo de 1 año después de finalizada dicha relación.

NO.	NOMBRE	CATEGORIA	ADSCRIPCIÓN	FIRMA
1	OMAR SANTIAGO CHAMPO	Enlace "D"	ÁREA DE APOYO ADMINISTRATIVO	
2	VICTOR MANUEL CHACON ROJAS	Enlace "D"	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA	
3	FABIAN HERNANDEZ CONSOSPO	Enlace "D"	ÁREA DE APOYO ADMINISTRATIVO	
4	GABRIELA GUADALUPE PEREZ HUERTA	Enlace "D"	DIRECCIÓN DE DISEÑO	
5	JESSICA ALEJANDRA SARMIENTO GALLEGOS	Enlace "D"	DIRECCIÓN DE DISEÑO	
6	SILKE PAMELA ZAMORA LÓPEZ	Enlace "D"	DIRECCIÓN DE DISEÑO	
7	ROGER GONZALEZ CHAVEZ	Enlace "D"	ÁREA DE APOYO ADMINISTRATIVO	
8	MIGUEL ANGEL YEPEZ MARTINEZ	Analista "G"	DIRECCIÓN DE DISEÑO	
9	ANA GABRIELA RAMOS PEREZ	Analista "G"	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA	
10	JOSE IVAN SANTIAGO LOPEZ	Enlace "D"	ÁREA DE APOYO ADMINISTRATIVO	
11	JUAN CARLOS CANCINO SANCHEZ	Enlace "D"	ÁREA DE APOYO ADMINISTRATIVO	
12	BELEM CALVO ESTRADA	Enlace "D"	DIRECCIÓN DE DISEÑO	
13	JOSE CARLOS RUIZ MARTINEZ	Analista "G"	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA	
14	JORGE ARTURO CALDERON FIGUEROA	Analista "G"	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA	
15	KAREN ORDOÑEZ FLORES	Analista "G"	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA	
16	PERLA ROMINA PIÑON SANCHEZ	Analista "G"	DIRECCIÓN DE DISEÑO	

NO.	NOMBRE	CATEGORIA	ADSCRIPCIÓN	FIRMA
17	JUAN EMMANUEL MIRANDA ALBARRAN	Analista "G"	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA	
18	AUREA MARTINEZ RUIZ	Analista "G"	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA	
19	VERONICA NATIVIDAD GARCIA BALLINAS	Analista "G"	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA	
20	JORGE ANGEL RAMIREZ ZUÑIGA	Analista "G"	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA	
21	OMAR SANTIAGO MONTERO	Analista "G"	ÁREA DE APOYO ADMINISTRATIVO	
22	ARLETTE CASTILLO TRINIDAD	Analista "G"	ÁREA DE APOYO ADMINISTRATIVO	
23	ROCIO JAQUELINE BARRIOS REYES	Analista "G"	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA	
24	FANNY RODRIGUEZ GÓMEZ	Aux. Adtvo. "C"	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA	
25	JOSE ALEXANDER DOMINGUEZ AREVALO	Aux. Adtvo. "C"	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA	
26	ANABEL COELLO SANTIAGO	Aux. Adtvo. "C"	DIRECCIÓN DE DISEÑO	
27	ANDREA CAROLINA GONZALEZ GOMEZ	Aux. Adtvo. "C"	DIRECCIÓN DE DISEÑO	
28	MARTHA ALICIA MAZA LOPEZ	Aux. Adtvo. "C"	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA	
29	MARÍA CANDELARIA JIMÉNEZ RODRÍGUEZ	Aux. Adtvo. "C"	DIRECCIÓN DE DISEÑO	
30	YURIDIA FAVIEL CERDA	Aux. Adtvo. "C"	DIRECCIÓN DE DISEÑO	
31	CARLOS DANIEL CRUZ MACIAS	Aux. Adtvo. "C"	DIRECCIÓN DE DISEÑO	
32	LUCERO GUADALUPE LOPEZ JONAPA	Aux. Adtvo. "C"	DIRECCIÓN DE DISEÑO	

NO.	NOMBRE	CATEGORIA	ADSCRIPCIÓN	FIRMA
33	MARIA JOSE CORDOVA SOLORZANO	Aux. Adtvo. "C"	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA	
34	MARIA CONCEPCION CRUZ LOPEZ	Aux. Adtvo. "C"	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA	
35	OLGA PATRICIA HERNANDEZ CHAVEZ	Aux. Adtvo. "C"	DIRECCIÓN DE DISEÑO	
36	YESENIA GUADALUPE LOPEZ CRUZ	Aux. Adtvo. "C"	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA	
37	MARIA GUADALUPE HERRERA PEREZ	Auxiliar Administrativo "B"	DIRECCIÓN GENERAL	
38	MARIA EUGENIA SANTIAGO CARPIO	Enlace A	DIRECCIÓN GENERAL	
39	VLADIMIR AGUILAR GOMEZ	Analista "G"	ÁREA DE APOYO ADMINISTRATIVO	
40	JAIME GOMEZ SANTIZ	Analista "G"	ÁREA DE APOYO ADMINISTRATIVO	
41	EDITH BECK CANO	Analista "G"	ÁREA DE APOYO ADMINISTRATIVO	
42	JULIO CESAR BERMUDEZ MAZARIEGOS	Mando Medio "E"	DIRECCIÓN DE DISEÑO	
43	HARRY WILLIAMS LOPEZ ZOMA	Analista "G"	DIRECCIÓN DE DISEÑO	
44	GUADALUPE IVONNE LEAL VAZQUEZ	Analista "G"	DIRECCIÓN DE DISEÑO	
45	GABRIELA ALEJANDRA SOLIS TOLEDO	Mando Medio "E"	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA	
46	YESSICA GUADALUPE NAVARRO ESPINOSA	Analista "G"	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA	
47	SUSANA ALEJANDRA CAMACHO LOPEZ			
48	MARLEN DEL ROSARIO ABRÓNIZ GÓMEZ			



**CENTRO ESTATAL DE PREVENCIÓN SOCIAL
DE LA VIOLENCIA Y PARTICIPACIÓN CIUDADANA**
Organismo Desconcentrado, jerárquicamente subordinado al Secretariado
Ejecutivo del Sistema Estatal de Seguridad Pública con plena autonomía administrativa

CENTRO ESTATAL
DE PREVENCIÓN SOCIAL
DE LA VIOLENCIA
Y PARTICIPACIÓN CIUDADANA
GOBIERNO DE CHIAPAS

Documento de Seguridad para la Protección de Datos Personales

CONTENIDOS

Considerandos.....	3
Definiciones.....	6
Objetivo y alcance del documento de seguridad.....	11
Responsabilidades del documento de seguridad.....	13
Sistema de Gestión de los datos personales.....	17
Inventario de tratamientos y datos personales.....	22
Análisis de Riesgo y Brecha.....	31
Programa de trabajo para la implementación de Medidas de Seguridad.....	36
Propuesta de capacitación en materia de datos personales.....	41

CONSIDERANDOS

Que la protección de los datos personales es un derecho humano consagrado en los artículos 6, base A y 16, segundo párrafo de la Constitución Política de los Estados Unidos Mexicanos, así como al acceso, rectificación, cancelación y oposición en los términos que determine la ley.

Que la LGPDPPSO define el documento de seguridad como el 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.

En este sentido la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas (LPDPPSOCHIS) establece un conjunto de bases principios y procedimientos que garantizan el derecho a la protección de los datos con carácter personal en posesión de sujetos obligados; entre los que figura el Centro Estatal de Prevención Social de la Violencia y Participación Ciudadana (CEPSVyPC) como Organismo Desconcentrado, jerárquicamente subordinado al Secretariado Ejecutivo del Sistema Estatal de Seguridad Pública con plena autonomía administrativa.

Que entre los objetivos de la LGPDPPSO se encuentra garantizar la observancia de los principios de protección de datos personales, proteger los datos personales en posesión de cualquier autoridad, así como promover, fomentar y difundir una cultura de protección de datos personales.

A partir de lo anterior, el **Documento de Seguridad** tiene como propósito establecer el marco de referencia de los parámetros que guían el tratamiento de los datos personales que se lleva a cabo al interior del Centro Estatal de Prevención Social de la Violencia y Participación Ciudadana del Estado de Chiapas (CEPSVyPC), por las diversas unidades administrativas que conforman su estructura orgánica, para mantener vigente y promover la

mejora continua en la protección de los mismos. Todo lo anterior, con base en el Artículo 45 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas y en términos de lo previsto en los artículos 35 y 36 de la LGPDPSO, además de desarrollar buenas prácticas en la materia.

En ese sentido, el CEPSPVyPC ha identificado los procesos que en el ámbito de su competencia involucran el tratamiento de datos personales, a efecto de mantener la seguridad de los mismos durante el ciclo de vida de la información, indicando la forma en la que se trata, las medidas de seguridad adoptadas y las áreas responsables de su protección, así como las finalidades del tratamiento de acuerdo a sus respectivos ámbitos de funciones, estableciendo líneas de acción como medidas de seguridad adoptadas a cada una de las áreas, a partir de las finalidades del tratamiento, con base en las funciones que desempeñan.

Considerando que los datos personales constituyen el principal activo de información objeto del presente documento, lo que se busca es crear un sistema de gestión para el tratamiento de los datos personales en posesión del CEPSPVyPC, que integre las acciones interrelacionadas como lo dispone el artículo 34 de la LGPDPSO, se entiende por sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, operar, monitorear, mantener y mejorar el tratamiento y seguridad de los datos personales.

Así, el CEPSPVyPC comprometido con la tutela de los datos personales que trata y en consonancia con la recomendación emitida por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), ha planteado acciones pertinentes para evitar la alteración, pérdida, transmisión y acceso no autorizados a los datos, mediante la implementación de medidas físicas, administrativas y técnicas, tendientes a garantizar la seguridad e integralidad de los mismos, así como su seguimiento y supervisión continuos.

Incluye además acciones que permitan controlar y verificar que el tratamiento de los datos personales se realice de acuerdo con los principios establecidos para la protección de los datos personales, implicando un compromiso con las disposiciones previstas en la ley y en los lineamientos generales, por parte de

los funcionarios involucrados; de ahí que dicho Sistema permita disponer de información relacionada con las medidas de seguridad, el análisis general de las amenazas y posibles vulnerabilidades, así como los mecanismos o acciones a implementar para mitigarlas.

Finalmente, ante la necesidad de mantener actualizado el documento de seguridad, se ha de procurar la mejora continua, a la actualización de los elementos que integran el documento de seguridad; las medidas de seguridad adoptadas en su tratamiento, ha propiciado la actualización de diversos elementos, tales como los inventarios de datos personales, las medidas de seguridad adoptadas con motivo de su tratamiento y el análisis de riesgo y brecha, con el objeto de monitorear e identificar posibles vulneraciones y mitigar los riesgos; además de avanzar en un proceso de sensibilización permanente respecto de la relevancia que tiene para la institución adoptar medidas correctivas y preventivas en función de los resultados obtenidos de la revisión de los sistemas de datos.

El presente documento se integra a partir de la gestión de actividades coordinadas para controlar y verificar que el tratamiento de los datos personales sea acorde con los principios que rigen su protección, pues para el CEPSVyPC la política de seguridad en esta materia constituye un compromiso con el cumplimiento de las disposiciones previstas tanto en la citada LGPDPPSO como en los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales) por parte de todos los involucrados.

Todo lo anterior, acompañado del desarrollo del programa de capacitación que permita comprender la importancia de adoptar medidas para la prevención de las vulneraciones a los datos personales.

DEFINICIONES

Áreas: Instancias de los sujetos obligados previstas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes, que cuentan o puedan contar, dar tratamiento, y ser responsables o encargadas de los datos personales.

Aviso de privacidad: Documento físico, electrónico o en cualquier otro formato generado por el responsable, que es puesto a disposición del titular con el objeto de informarle los propósitos principales del tratamiento al que serán sometidos sus datos personales.

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

Bloqueo: La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabadas, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su supresión en la base de datos, archivo, registro, expediente o sistema de información que corresponda.

Comité de Transparencia: Instancia a que se refiere el artículo 51 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas.

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.

Consentimiento: Manifestación de la voluntad libre, específica e informada del titular, mediante la cual autoriza el tratamiento de sus datos personales.

Datos personales: Cualquier información concerniente a una persona física identificada o identificable expresada en forma numérica, alfabética, alfanumérica, gráfica, fotográfica, acústica o en cualquier otro formato. Se considera que una persona es identificable cuando su identidad puede determinarse directa o indirectamente a través de cualquier información.

Datos personales sensibles: Aquellos que se refieren a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. Se consideran sensibles, de manera enunciativa más no limitativa, los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud pasado, presente o futuro, creencias religiosas, filosóficas y morales, opiniones políticas, datos genéticos, datos biométricos y preferencia sexual.

Derechos ARCO: Los derechos de acceso, rectificación, cancelación y oposición de datos personales, así como la oposición al tratamiento de los mismos.

Días: Días hábiles.

Disociación: El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo.

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

Encargado: Prestador de servicios, que con el carácter de persona física o jurídica pública o privada, ajena a la organización del responsable, trata datos personales a nombre y por cuenta de éste.

Evaluación de impacto a la protección de datos personales: Documento mediante el cual se valoran y determinan los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar, prevenir y mitigar posibles riesgos que puedan comprometer el cumplimiento de los principios, deberes, derechos y demás obligaciones previstas en la presente Ley y demás normatividad aplicable en la materia.

Fuentes de acceso público: Aquellas bases de datos, sistemas o archivos que por disposición de ley puedan ser consultadas públicamente cuando no exista impedimento por una norma limitativa y sin más exigencia que, en su caso, el pago de una contraprestación, tarifa o contribución. No se considerará fuente de acceso público cuando los datos personales contenidos en la misma sean obtenidos o tengan una procedencia ilícita, conforme a las disposiciones establecidas por la presente Ley y demás normatividad que resulte aplicable.

Instituto: El Instituto de Acceso a la Información Pública del Estado de Chiapas.

Instituto Nacional: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Ley: Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.

Ley de Transparencia: Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas.

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

Ley General de Transparencia: Ley General de Transparencia y Acceso a la Información Pública.

Medidas compensatorias: Mecanismos alternos para dar a conocer a los titulares el aviso de privacidad, a través de su difusión por medios masivos de comunicación u otros de amplio alcance.

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 procedimientos para la gestión, soporte y revisión de la seguridad de los datos personales a nivel organizacional, la identificación, clasificación y borrado seguro de los datos personales, así como la sensibilización y capacitación del personal en materia de protección de datos personales.

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. De manera enunciativa más no limitativa, se deberán considerar las siguientes actividades:

a) Prevenir el acceso no autorizado al perímetro de la organización del responsable, sus instalaciones físicas, áreas críticas, recursos y datos personales.

b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización del responsable, recursos y datos personales.

c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pudiera salir de la organización del responsable, y

d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

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 los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deberán considerar las siguientes actividades:

- a) Prevenir que el acceso a los datos personales, así como a los recursos, sea por usuarios identificados y autorizados;
 - b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
 - c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y
 - d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales;
- Plataforma Nacional:** Plataforma Nacional de Transparencia a que se refiere el artículo 49 de la Ley General de Transparencia y Acceso a la Información Pública.

Remisión: Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, con independencia de que se realice dentro o fuera del territorio mexicano.

Responsable: Cualquier autoridad, dependencia, entidad, órgano y organismos de los poderes Legislativo, Ejecutivo y Judicial, ayuntamientos, órganos constitucionales autónomos, fideicomisos y fondos públicos y partidos políticos locales, que decide y determina los fines, medios y demás cuestiones relacionadas con determinado tratamiento de datos personales.

Sistema Nacional: Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Supresión: La baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable.

Titular: La persona física a quien corresponden los datos personales.

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

Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados aplicados a los datos personales, relacionadas, de manera enunciativa más no limitativa, con la obtención, uso, registro, organización, conservación, elaboración, utilización, estructuración, adaptación, modificación, extracción, consulta, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, transferencia y en general cualquier uso o disposición de datos personales.

Unidad de Transparencia: Instancia a que se refiere el artículo 56 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas, y

Sistema de Gestión: Se entenderá por sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, de conformidad con lo previsto en la presente Ley y las demás disposiciones que le resulten aplicables en la materia.

OBJETIVO Y ALCANCE DEL DOCUMENTO DE SEGURIDAD

1. Objetivos del Documento de Seguridad

El presente documento tiene como objetivo: ofrecer el marco de trabajo necesario para la protección de los datos personales en posesión del Centro Estatal de Prevención Social de la Violencia y Participación Ciudadana, como un medio para cumplir con las obligaciones que establece la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de Chiapas y los Lineamientos Generales, así como la normatividad que derive de los mismos; estableciendo con ello, los elementos y actividades de gestión para la operación y control de los procesos que impliquen el tratamiento de datos personales, a efecto de protegerlos de manera sistemática y continua, y promover la adopción de mejores prácticas en relación con la protección de datos personales, así como establecer los principales elementos que integran las medidas de seguridad administrativas, físicas y técnicas que ha adoptado el CEPSVyPC para garantizar la confidencialidad, integridad y disponibilidad de los datos personales; así como determinar las posibles vulnerabilidades, amenazas y riesgos de los que pueden ser objeto en un plano general los diversos sistemas de información y procesos en los se tratan datos personales por las diversas unidades administrativas, conforme a lo establecido en la LGPDPPSO y a los Lineamientos Generales.

2. Alcance del Documento de Seguridad

El documento de seguridad aplica a todas las unidades administrativas que realicen tratamientos de datos personales en ejercicio de sus atribuciones, y a todos los tratamientos de datos personales que efectúen, mismos que se encuentran bajo su estricta responsabilidad, tanto en los espacios físicos como los medios electrónicos en los que los resguardan, operan y administran, con observancia de los principios, deberes y obligaciones que establece la ley.

Quedan exceptuados de la aplicación de este programa, los datos personales que correspondan al cumplimiento de las obligaciones de transparencia a las que refieren el artículo 18 de la Ley de Transparencia y Acceso a la Información Pública del estado de Chiapas.

Las unidades administrativas que forman parte del Centro Estatal de Prevención Social de la Violencia y Participación Ciudadana y que deberán observar el Programa de Protección de Datos Personales son las siguientes:

- Dirección General
- Dirección de Participación Ciudadana en la Prevención Social de la Violencia
- Área de Apoyo Administrativo

En este sentido, la Dirección de Diseño, Planeación y Seguimiento de Políticas Públicas en Prevención Social integra este documento de seguridad con base en la información generada por las citadas unidades administrativas acorde al ámbito de sus funciones y de conformidad con las disposiciones jurídicas aplicables.

RESPONSABILIDAD DEL DOCUMENTO DE SEGURIDAD

Para efectos del presente documento, la normatividad aplicable es la siguiente:

- Constitución Política de los Estados Unidos Mexicanos, última reforma publicada en el Diario Oficial de la Federación el 28 de mayo 2021.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el Diario Oficial de la Federación el 26 de enero de 2017.
- Fracciones V, VI y VII del artículo 42 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP)
- Fracciones VI, VII y IX del artículo 27 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas (LTAIPCHIS)
- Fracciones IV, XII y XIV del artículo 91 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO)
- Fracciones VIII, XVI, XXI y XXIII del artículo 121 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas (LPDPPSOCHIS)
- Artículo 6 inciso A y 16 segundo párrafo de la Constitución Política de los Estados Unidos Mexicanos
- Artículo 5 de la Constitución Política del Estado Libre y Soberano del Estado de Chiapas
- Marco jurídico señalado en el artículo 7 fracción I inciso A y 14 fracciones VI y X del Reglamento Interior de este Centro Estatal de Prevención Social de la Violencia y Participación Ciudadana (CEPSVyPC)
- Artículo 5º del Decreto de Creación por el que se crea el Centro Estatal de Prevención Social de la Violencia y Participación Ciudadana
- En términos de las disposiciones previstas en la Ley de los Derechos de Niñas, Niños y Adolescentes del Estado de Chiapas y demás ordenamientos que resulten aplicables.
- Con fundamento en lo dispuesto por el artículo 44 de la LPDPPSOCHIS, que señala que entre los mecanismos que deberá adoptar el responsable para cumplir con el principio de responsabilidad establecido en la presente Ley están, al menos, los siguientes:

- I. En la medida de sus posibilidades presupuestales destinar recursos para la instrumentación de programas y políticas de protección de datos personales.
 - II. Elaborar políticas y programas de protección de datos personales obligatorios y exigibles al interior de la organización del responsable.
 - III. Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales.
 - IV. Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran.
 - V. Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.
 - VI. Establecer procedimientos para recibir y responder dudas y quejas de los titulares.
 - VII. En la medida de sus posibilidades diseñar, desarrollar e implementar sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la presente Ley y las demás que resulten aplicables en la materia, y;
 - VIII. Garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, cumplan por defecto con las obligaciones previstas en la presente Ley y las demás que resulten aplicables en la materia.
- El responsable deberá revisar las políticas, los programas de seguridad y las políticas de procedimientos de control a que se refieren las fracciones IV y V del presente artículo, respectivamente, al menos cada dos años, así como actualizarlas cuando al tratamiento de datos personales se le realicen modificaciones sustanciales.

- Con fundamento en lo dispuesto por el artículo 45 de la LPDPPSOCHIS, que señala, con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

Lo anterior, sin perjuicio de lo establecido por las disposiciones vigentes en materia de seguridad, emitidas por las autoridades competentes al sector que corresponda, cuando éstas contemplen una protección mayor para el titular o complementen lo dispuesto en la presente Ley y demás normativa aplicable.

- Con fundamento en lo dispuesto por el artículo 46 de la LPDPPSOCHIS, que señala, las medidas de seguridad adoptadas por el responsable deberán considerar:

- I. El riesgo inherente a los datos personales tratados.
- II. La sensibilidad de los datos personales tratados.
- III. El desarrollo tecnológico.
- IV. Las posibles consecuencias de una vulneración para los titulares.
- V. Las transferencias de datos personales que se realicen.
- VI. El número de titulares, y
- VII. Las vulneraciones previas ocurridas en los sistemas de tratamiento.

- Con fundamento en lo dispuesto por el artículo 47 de la LPDPPSOCHIS, que señala, que para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable en la medida de sus posibilidades deberá realizar, al menos, las siguientes actividades interrelacionadas:

- I. Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión.
- II. Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales.
- III. Elaborar un inventario de los datos personales y/o sistemas de

tratamiento.

IV. Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros.

V. Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable.

VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales.

VII. Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, y

VIII. Diseñar y aplicar diferentes niveles de capacitación de su personal, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

SISTEMA DE GESTIÓN DE LOS DATOS PERSONALES

1. Desarrollo de la política de gestión

El sistema de gestión de datos personales es el medio por el cual el Centro Estatal de Prevención Social de la Violencia y Participación Ciudadana (CEPSVyPC) garantiza el tratamiento de los datos personales que lleva a cabo como parte de sus funciones, desde su obtención, uso, registro, conservación, acceso, manejo, aprovechamiento, transferencia, disposición o cualquier otra operación correspondiente; para lo cual, se establecen políticas y métodos orientados a salvaguardar la confidencialidad, integridad y disponibilidad de estos datos, de acuerdo con Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados del estado de Chiapas y la Ley General de Transparencia y Acceso a la Información Pública del estado de Chiapas.

En tal virtud, se inició un proceso de organización y planificación de los esquemas de protección de datos personales, tomando como punto de partida la identificación de los procesos y tareas en los que, de acuerdo con el ámbito de funciones de las distintas áreas que conforman el Centro, se involucra el tratamiento de ese tipo de datos.

Para tal fin, se elaboró un formulario que facilitó a cada unidad administrativa, la identificación de los inventarios que llevan a cabo como parte de su responsabilidad, considerando lo establecido en el artículo 47 de la Ley de Protección de Datos Personales del Estado de Chiapas y considerando los elementos mínimos que establece el artículo 33, fracción II, de la Ley General y el diverso 58 de los Lineamientos Generales, logrando con ello el desarrollo de un instrumento homogéneo y estandarizado se llevó a cabo el levantamiento del **inventario de datos**, tratando de identificar, entre otros aspectos, la categoría y tipo de datos que son sometidos a tratamiento, incluyendo los de carácter sensible.

Los medios a través de los cuales se obtienen dichos datos, el sistema físico y/o electrónico que se utiliza para su acceso, manejo, aprovechamiento, monitoreo y procesamiento, las características del lugar donde se ubican las bases físicas o electrónicas de datos, las finalidades del tratamiento, y el nombre, cargo y adscripción de los servidores públicos que tienen acceso a la operación sobre esos datos, además de si son objeto de la transferencia y la identificación de los destinatarios o receptores de los mismos, así como las causas que la justifican.

En este mismo sentido, el inventario ha contribuido desde el punto operativo a considerar el ciclo de vida de los datos personales, de forma tal que los servidores públicos que intervienen en el tratamiento conocen que, una vez concluida la finalidad de los datos, éstos deben ser sometidos a un proceso de bloqueo y, en su caso, de cancelación, supresión o destrucción, lo que cobra especial relevancia en el marco del proceso de baja documental que las áreas realizan conforme a las disposiciones que regulan la gestión documental al interior del Centro.

De igual forma, una vez integrados los inventarios de tratamientos y de datos, se dispuso de una metodología para la elaboración del análisis de riesgos, en la cual, atendiendo a lo previsto en el artículo 33, fracción IV, de la Ley General de la materia, las áreas responsables de su tratamiento identificaron el valor de los datos personales de acuerdo con su categoría y el ciclo de vida; el valor de exposición de los activos involucrados en el tratamiento; las consecuencias que pueden generarse para los titulares de los mismos con motivo de su posible vulneración y/o uso indebido y los factores de riesgo a los que podrían encontrarse expuestos por medidas de seguridad poco confiables.

Lo anterior, permitió identificar la brecha entre las medidas de seguridad existentes y las medidas de seguridad faltantes para que garanticen la seguridad de los datos, además de promover el reconocimiento de las medidas de seguridad administrativas, entendidas como el conjunto de políticas y procedimientos de gestión, soporte y revisión de la seguridad de la información;

físicas, que corresponden a las acciones o mecanismos para proteger el entorno físico de los datos, así como de los recursos involucrados en su tratamiento, así como **técnicas** que se valen de la tecnología para proteger el entorno digital de la información, también se han registrado nuevas medidas de seguridad que deberán desarrollarse para fortalecer algunos de los controles que actualmente son implementados; es decir, el análisis de brecha a partir del cual será posible mitigar los riesgos a los que están expuestos los datos tratados.

A partir de esta identificación de posibles vulneraciones es factible prevenir posibles debilidades en la seguridad de los datos y las áreas de oportunidad, aun cuando no haya existido un daño real, mediante la:

- Identificación de la ineficiencia de los controles de accesos físicos y electrónicos.
- Inadecuada administración de autorizaciones de accesos a los datos personales (sistemas de privilegio).
- Deficiente conocimiento de procesos y responsabilidades en materia de protección de datos personales.
- Falta de definición de perfiles y roles para delimitar funciones manejo y uso de datos.
- Falta de seguimiento y monitoreo a los medios de seguridad.
- La inexistencia de mecanismos para garantizar la confidencialidad.

Aunado a las anteriores vulnerabilidades, de manera enunciativa más no limitativa, se examinan algunos tipos de amenazas, que pueden ser intencionales o no, a las que podría enfrentarse la institución y sus activos de información.

- Robo, extravío o copia no autorizada
- Uso, acceso o tratamiento no autorizado
- Daño, alteración o modificación no autorizada
- Pérdida o destrucción no autorizada
- Otras.

El riesgo que de manera general puede presentarse en caso de que las amenazas señaladas exploten las vulnerabilidades, es el de facilitar el acceso a los datos personales de manera no autorizada con el fin de comprometer su confidencialidad, disponibilidad e integridad, por lo que las medidas de seguridad por parte de las áreas comisionadas están orientadas a proteger los datos personales.

A partir de la identificación de vulnerabilidades y amenazas se han establecido medidas de seguridad generales que, de acuerdo a la experiencia y mejores prácticas, son monitoreadas para lograr la mejora continua por parte de todos los involucrados en el tratamiento.

En el marco del sistema de gestión y política de seguridad institucional, se procurará:

- Identificar a los servidores públicos del CEPSVyPC responsables del tratamiento de los datos personales.
- Que los tratamientos de datos personales estén sujetos al principio de consentimiento siempre que la Ley lo permita.
- Velar por el cumplimiento de los principios, estableciendo y manteniendo medidas de seguridad y de confidencialidad durante el ciclo de vida de los datos personales, en estricto respeto de los derechos de los titulares.
- Tratar datos personales de manera lícita, conforme a las disposiciones establecidas por la Ley General.
- Informar a los titulares del tratamiento de los datos y sus finalidades.
- Procurar que los datos personales tratados sean correctos y estén actualizados.
- Suprimir los datos personales cuando hayan dejado de ser necesarios para las finalidades para las cuales se obtuvieron.
- Tratar los datos personales estrictamente para propósitos legales o legítimos del CEPSVyPC.
- No obtener datos personales a través de medios fraudulentos.
- Tratar estrictamente los datos personales necesarios, adecuados y relevantes en relación con las finalidades.

- Guardar la confidencialidad de los datos personales.
- Mantener actualizado el inventario de datos personales o de las categorías que maneja el CEPSVyPC.
- Respetar los derechos de los titulares en relación con sus datos personales.
- Aplicar las excepciones contempladas en la normativa en materia de protección de datos personales.

Buscando el logro de lo anterior, y tomando como punto de partida la identificación de vulnerabilidades y amenazas, se han establecido medidas de seguridad generales, que, de acuerdo con otras experiencia y mejores prácticas tomadas como referencia, se encaminan a la mejora continua por parte de las personas involucradas en el tratamiento, en la búsqueda de lograr la salvaguarda del derecho a la privacidad y protección de datos personales, se han determinado las líneas de acción para el personal encargado de tratamiento de datos, con el propósito de generar mecanismos para el resguardo adecuado, actuando en apego a la LPDPPSO de Chiapas y los lineamientos correspondientes.

INVENTARIO DE TRATAMIENTOS Y DATOS PERSONALES

Para cumplir con los objetivos y obligaciones que prevé la LPDPPSO de Chiapas y la LGPDPPSO, particularmente en materia de seguridad y, como parte del debido cumplimiento de las obligaciones es necesario que cada una de las unidades administrativas realicen un diagnóstico de los tratamientos de datos personales que llevan a cabo, a fin de identificar los procesos en los que actualmente se lleva a cabo tratamiento de datos personales, el diagnóstico en mención se basa en la elaboración de un inventario con la información básica de cada tratamiento de datos personales que se realizan en el Centro Estatal de Prevención Social de la Violencia y Participación Ciudadana.

Por **inventario de tratamiento de datos personales** se entenderá el control documentado que se llevará del conjunto de operaciones de los tratamientos que realizan las áreas que integran el CEPSPVyPC, con motivo de los datos que se recaban de las personas, a través de procedimientos automatizados o físicos, que van desde su obtención, registro, organización, conservación, utilización, cesión, difusión, interconexión, hasta la rectificación, cancelación y oposición, con motivo de la atención del ejercicio de éstos derechos en el ámbito de sus atribuciones.

Así, en coordinación con las áreas, como resultado del proceso de análisis y actualización de la información, se logró identificar a las unidades administrativas que realizan tratamientos con datos personales; y estas son:

- Dirección General
- Dirección de Diseño, Planeación y Seguimiento de Políticas Públicas en Prevención Social
- Dirección de Participación Ciudadana en la Prevención Social de la Violencia
- Área de Apoyo Administrativo

Estos tratamientos se realizan en absoluto apego a sus funciones, a través de las diversas áreas que las integran y permiten el desarrollo de los procesos que realizan para el cumplimiento de dichas funciones.

En relación con lo anterior, fue posible identificar 73 procesos que se desarrollan, que implican el tratamiento de datos personales. Mismas que a continuación se describen:

Dirección o Área administrativa	Área o Departamento	Proceso o tratamiento
Dirección General	Dirección General	Visitas Oficiales a la Titular del CEPVPC
Dirección de Participación Ciudadana en la Prevención Social de la Violencia	Dirección de Participación Ciudadana en la Prevención Social de la Violencia	Comités de Consulta y Participación Ciudadana (Municipales)
		Enlaces con los Coordinadores Municipales de Prevención del Delito, para recepción de información e integración del plan anual de trabajo
		Programa Ocupando mi comunidad (FASP 2022)
		Programa Emprende Aprendiendo (FASP y Gasto Institucional 2022)
		Programa Vecino Vigilante (Gasto Institucional 2022)
		Diplomado en Línea "Prevención de las Violencias y Fortalecimiento de la Seguridad Ciudadana", de la Fundación Carlos Slim
		Sistema Institucional de Archivos
		Jornadas de Prevención (Pláticas, talleres, capacitaciones, cine de prevención, recuperación de espacios públicos)

Dirección o Área administrativa	Área o Departamento	Proceso o tratamiento
Dirección de Diseño, Planeación y Seguimiento de Políticas Públicas en Prevención Social	Dirección de Diseño, Planeación y Seguimiento de Políticas Públicas en Prevención Social	Atención y Seguimiento de Solicitudes de Información
		Auditorías
		Capacitaciones a los Beneficiarios de los Apoyos de Beneficencia Pública
		Capacitaciones en Instituciones Educativas
		Comisionada y Comisionado Infantil 2022
		Concurso Virtual Los Ritmos de Mi Tierra
		Deporte Preventivo
		Diplomado en Prevención Social de la Violencia y la Delincuencia
		Escuela con Valores
		Escuelita Preventiva
		Informes Mensuales y Trimestrales de los Coordinadores de Prevención del Delito Municipales
		Juega Vive
		Mujeres Constructoras de Paz
		Diplomado Prevención de la Violencia Familiar

Dirección o Área administrativa	Área o Departamento	Proceso o tratamiento
Área de Apoyo Administrativo	Área de Apoyo Administrativo	Elaboración de nómina
		Pago de nómina
		Trámite y pago de impuestos
		Expedientes de personal
		Timbrado de nómina
		Sistema NECH
		Movimientos nominales
		Expedición de constancias y credenciales
		Retención de pago de nómina o bloqueo de cuenta
		Elaboración y actualización de las declaraciones patrimoniales
		Elaboración de listado para alta y baja de Infonavit e Imss
		Elaboración de listado para seguro de vida
		Control y seguimiento de asistencia del personal
		Solicitud de cartas de autorización para el depósito de nómina
		Elaboración de contratos de personal
		Elaboración de actas de extrañamiento y administrativas
		Trámite de solicitud de volante de validación



**CENTRO ESTATAL DE PREVENCIÓN SOCIAL
DE LA VIOLENCIA Y PARTICIPACIÓN CIUDADANA**
Organismo Desconcentrado, jerárquicamente subordinado al Secretariado
Ejecutivo del Sistema Estatal de Seguridad Pública con plena autonomía administrativa

CENTRO ESTATAL
DE PREVENCIÓN SOCIAL
DE LA VIOLENCIA
Y PARTICIPACIÓN CIUDADANA
GOBIERNO DE CHIAPAS

		Informe de Gobierno
--	--	---------------------

Dirección o Área administrativa	Área o Departamento	Proceso o tratamiento
Área de Apoyo Administrativo	Área de Apoyo Administrativo	Registro de avance de metas en el SISAI, SITEC y NUMERALIA
		Informe SISGAB
		COCODI
		Recepción y trámite de facturas
		Resguardos vehiculares y mobiliario
		Entrada y salida de almacén
		Publicaciones en medios de difusión y comunicación social
		Videos en medios de difusión y comunicación social
		Boletines e información en medios masivos de comunicación
		Elaboración de contratos
		Elaboración de convenios de colaboración
		Certificaciones de documentos
		Elaboración de actas



CHIAPAS
GOBIERNO

**CENTRO ESTATAL DE PREVENCIÓN SOCIAL
DE LA VIOLENCIA Y PARTICIPACIÓN CIUDADANA**
Organismo Desconcentrado, jerárquicamente subordinado al Secretariado
Ejecutivo del Sistema Estatal de Seguridad Pública con plena autonomía administrativa

CENTRO ESTATAL
DE PREVENCIÓN SOCIAL
DE LA VIOLENCIA
Y PARTICIPACIÓN CIUDADANA

GOBIERNO DE CHIAPAS

		Seguimiento a procedimientos administrativos, amparos, juicios de la dependencia y contra la dependencia y procesos seguidos en forma de juicio
--	--	---

Dirección o Área administrativa	Área o Departamento	Proceso o tratamiento
Área de Apoyo Administrativo	Área de Apoyo Administrativo	Trámite de pago a proveedores y prestadores de servicios
		Subcomité de Adquisiciones, Arrendamiento de Bienes Muebles y Contratación de Servicios del CEPSVyPC
		Análisis funcional de la cuenta pública del Centro
		Anteproyecto de Presupuesto de Egresos del Gasto Institucional e Inversión
		Trámite de validación y autorización de los recursos de inversión ante la SH del Estado
		Validación de proyectos de inversión ante el Comité Sectorial de Seguridad y Estado de Derechos de la SSyPC
		Trámite de pago de viáticos



**CENTRO ESTATAL DE PREVENCIÓN SOCIAL
DE LA VIOLENCIA Y PARTICIPACIÓN CIUDADANA**
Organismo Desconcentrado, jerárquicamente subordinado al Secretariado
Ejecutivo del Sistema Estatal de Seguridad Pública con plena autonomía administrativa

CENTRO ESTATAL
DE PREVENCIÓN SOCIAL
DE LA VIOLENCIA
Y PARTICIPACIÓN CIUDADANA
GOBIERNO DE CHIAPAS

		Reporte de entrega de Ayudas Sociales
		Informar sobre el pago, retención, acreditamiento y traslado del IVA (DIOT)
		Elaboración del informe contable y presupuestal mensual

Dirección o Área administrativa	Área o Departamento	Proceso o tratamiento
Área de Apoyo Administrativo	Área de Apoyo Administrativo	Elaboración de la Cuenta Pública Financiera y Presupuestal
		Elaboración del Informe del Fondo de Aportaciones para la Seguridad Pública FASP 2022
		Realizar encuesta en el Sistema de Evaluación de la Armonización Contable (SEvAC) del CEPSVyPC
		Conciliaciones bancarias y ministrados
		Adecuación Presupuestal de Gasto Institucional y de Inversión
		Envío de flujo de efectivo de los pagos realizados de manera mensual al área de coordinación administrativa de la Secretaría de Hacienda

Como resultado del proceso de análisis, se identificaron también los datos personales utilizados en los tratamientos,



mismos que corresponden a las tres categorías, tal como se señala a continuación:

De identificación

- Nombre, domicilio, CURP, fotografía, huella digital, edad, clave de elector, estado civil, RFC, correo electrónico personal, teléfono, sexo, información académica, fecha y lugar de nacimiento, cédula profesional, número de seguridad social, antecedentes laborales, beneficiarios, número de licencia de conducir, currículum vitae, datos de identificación, nacionalidad, ocupación, sexo y títulos profesionales.

Patrimoniales

- Cuentas bancarias, CLABE interbancaria, institución bancaria, facturas, descuentos personales (ahorro voluntario, hipoteca, seguro médico, seguro de automóvil, etc.) estados financieros, información fiscal, información financiera, saldos, propiedades y pensión alimenticia.

Sensibles

- Datos de salud, diagnóstico médico, antecedentes médicos, tipo de sangre, datos biométricos, antecedentes penales y resultados de evaluación psicométrica y de valores.

A partir de lo anterior, el Inventario de Datos Personales del CEPVPC posibilitó la identificación de hallazgos en relación con el tratamiento de datos personales, aportando los elementos que permiten focalizar las áreas con mayor incidencia en el tratamiento de éstos y, con ello, enfocar los trabajos de atención para el cumplimiento de las disposiciones jurídicas en materia de protección de datos.

Sobre el particular, se identificó que por lo que hace al tratamiento de datos de **identificación**, en 3 unidades administrativas aludidas se llevan a cabo tratamientos de datos de esta naturaleza; por lo que hace a los **patrimoniales** en 1 de ellas se realiza tratamiento de éstos, y por los que hace a los **sensibles**, únicamente en 1 unidad administrativa trata este tipo de datos.



CHIAPAS
GOBIERNO DEL ESTADO

Ante este contexto, es dable concluir que el Inventario de Datos Personales del Centro Estatal de Prevención Social de la Violencia y Participación Ciudadana, a partir de los hallazgos identificados en su actualización, se constituye como un elemento del Sistema de Gestión de Datos Personales, que junto con las medidas de seguridad representa un instrumento de evidencia para la implementación de las directrices de la Política en materia de protección de datos personales.

Asimismo, delinea las rutas para una capacitación focalizada en materia protección de datos en aras de fortalecer la estructura de los operadores en cada uno de los procesos en que se tratan datos, buscando con ello sensibilizar y preparar a los responsables y encargados de los mismos para que su tratamiento se lleve a cabo de conformidad con los estándares estatales, nacionales e internacionales en la materia.

En tal virtud, el Inventario de Datos Personales del CEPVPC se inscribe como un elemento más de la política para el cumplimiento de las directrices determinadas por la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas (LPDPPSOCHIS) y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, aportando con ello certeza a la ciudadanía de cuáles son y cuál es el destino de los datos recabado por éste ente de Prevención.

ANÁLISIS DE RIESGO Y BRECHA

De acuerdo con el artículo 50 de la LPDPPSOCHIS, el análisis de riesgo y de brecha forma parte del documento de seguridad, como un medio para identificar las medidas de seguridad implementadas y, en relación con ello, las amenazas de vulneración en que se encuentran los datos personales.

El análisis sirve para identificar el riesgo inherente a los datos personales en el tratamiento a que son sometidos en el ejercicio de las funciones del Centro Estatal de Prevención Social de la Violencia y Participación Ciudadana, con respeto a la integridad de las personas.

La evaluación de riesgos de los datos personales forma parte de la serie de elementos que integran el documento de seguridad, cuyo propósito es garantizar la confidencialidad, integridad y disponibilidad de los datos personales en posesión del CEPSVyPC.

Asimismo, para el análisis de riesgo se han tomado en cuenta lo establecido en el lineamiento para la protección de datos personales del estado de Chiapas, que en su artículo 55, define que para el cumplimiento al artículo 47 fracción IV de la Ley Estatal, el responsable deberá realizar un análisis de riesgo de los datos personales tratados considerando lo siguiente:

I. Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico;

II. El valor de los datos personales de acuerdo con su clasificación previamente definitiva y su ciclo de vida;

III. El valor y exposición de los activos involucrados en el tratamiento de los datos personales;

IV. Las consecuencias y negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida; y

V. Los factores previstos en el artículo 47 de la Ley Estatal.

Bajo esta premisa, para analizar los riesgos de los datos personales que son objeto de tratamiento por el CEPSVPC, se aplicó un instrumento para, primeramente, clasificar los datos utilizados, a partir de la categorización existente en la ley:

1) De identificación o contacto, que se refieren a información por la que se identifica a una persona y/o permiten su contacto como, por ejemplo, el nombre, el domicilio, el correo electrónico, la firma, los usuarios, el Registro Federal de Contribuyentes, la Clave Única de Registro de Población o la edad.

2) Patrimoniales, que comprenden la información que se encuentran vinculados al patrimonio de una persona como, por ejemplo, el salario, los créditos, las tarjetas de débito, los cheques o las inversiones.

3) Sensibles, que consideran la información concerniente a la esfera más íntima de su titular o que su uso puede dar origen a discriminación o conlleva un riesgo grave para éste como, por ejemplo, el origen étnico, el estado de salud presente o futuro, las creencias religiosas, la opinión política o la orientación sexual.

De los anteriores, se identificó que se trabaja sobre todo con dos categorías: datos de identificación y datos patrimoniales, ya que como datos sensibles solamente se recuperan datos de salud.



CHIAPAS
GOBIERNO DEL ESTADO

**CENTRO ESTATAL DE PREVENCIÓN SOCIAL
DE LA VIOLENCIA Y PARTICIPACIÓN CIUDADANA**
Organismo Desconcentrado, jerárquicamente subordinado al Secretariado
Ejecutivo del Sistema Estatal de Seguridad Pública con plena autonomía administrativa

CENTRO ESTATAL
DE PREVENCIÓN SOCIAL
DE LA VIOLENCIA
Y PARTICIPACIÓN CIUDADANA
GOBIERNO DE CHIAPAS

En un segundo momento, para la determinación del riesgo sobre esa tipología de datos personales se valoró la probabilidad e impacto de que, en su obtención, almacenamiento, tratamiento, transferencia o remisión, bloqueo y/o eliminación (ciclo de vida), en correspondencia con la cantidad de datos involucrados, se materialice uno o más factores que pueden causar un daño a su titular (amenaza).

Para el desarrollo del análisis, se recuperaron cuatro tipos de amenazas sustentados en la Ley:

- Robo, extravío o copia no autorizada.
- Uso, acceso o tratamiento no autorizado.
- Daño, alteración o modificación no autorizada.
- Pérdida o destrucción no autorizada.

A partir de lo anterior, se consideró una probabilidad baja, media o alta de que la amenaza suceda en las distintas etapas de vida y tipo de datos personales.

Además, se tomó en cuenta la consecuencia desfavorable que podría sufrir el titular en caso de vulneración, la cual que puede ser leve, moderada o grave.

En cuanto a la valoración del riesgo por el tipo de dato en cada proceso en el que las unidades administrativas del CEPSVyPC tratan datos personales, se señaló una escala del 0 al 3, representándose de la forma siguiente:

TIPO DE DATO	RIESGO INHERENTE	NIVEL DE RIESGO
Datos identificativos	Bajo	1

Datos electrónicos, de domicilio laborales, patrimoniales, procedimientos administrativos	Medio	2
Datos sensibles	Medio	3

Análisis de la Información

Como resultado del levantamiento de información para el análisis de riesgo y de brecha, se identifica que el CEPSVyPC cuenta con 4 unidades administrativas en las que tienen lugar tratamientos de datos personales para el desarrollo de los 71 procesos como se ilustra a continuación:

Dirección General

- 1 tratamiento

Dirección de Participación Ciudadana en la Prevención Social de la Violencia

- 8 tratamientos

Dirección de Diseño, Planeación y Seguimiento de Políticas Públicas en Prevención Social

- 14 tratamientos

Área de Apoyo Administrativo

- 48 tratamientos

De los cuales 44 funcionarios manejan datos personales, anexo cuadro con nombre del servidor público, área de adscripción y cargo.



**CENTRO ESTATAL DE PREVENCIÓN SOCIAL
DE LA VIOLENCIA Y PARTICIPACIÓN CIUDADANA**
Organismo Desconcentrado, jerárquicamente subordinado al Secretariado
Ejecutivo del Sistema Estatal de Seguridad Pública con plena autonomía administrativa

**CENTRO ESTATAL
DE PREVENCIÓN SOCIAL
DE LA VIOLENCIA
Y PARTICIPACIÓN CIUDADANA**
GOBIERNO DE CHIAPAS

NO.	NOMBRE	CATEGORIA	ADSCRIPCIÓN
1	OMAR SANTIAGO CHAMPO	Enlace "D"	ÁREA DE APOYO ADMINISTRATIVO
2	VICTOR MANUEL CHACÓN ROJAS	Enlace "D"	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA EN LA PREVENCIÓN SOCIAL DE LA VIOLENCIA
3	FABIÁN HERNÁNDEZ CONSOSPO	Enlace "D"	ÁREA DE APOYO ADMINISTRATIVO
4	GABRIELA GUADALUPE PÉREZ HUERTA	Enlace "D"	DIRECCIÓN DE DISEÑO, PLANEACIÓN Y SEGUIMIENTO DE POLÍTICAS PÚBLICAS EN PREVENCIÓN SOCIAL
5	JESSICA ALEJANDRA SARMIENTO GALLEGOS	Enlace "D"	DIRECCIÓN DE DISEÑO, PLANEACIÓN Y SEGUIMIENTO DE POLÍTICAS PÚBLICAS EN PREVENCIÓN SOCIAL
6	SILKE PAMELA ZAMORA LÓPEZ	Enlace "D"	DIRECCIÓN DE DISEÑO, PLANEACIÓN Y SEGUIMIENTO DE POLÍTICAS PÚBLICAS EN PREVENCIÓN SOCIAL
7	ROGER GONZÁLEZ CHÁVEZ	Enlace "D"	ÁREA DE APOYO ADMINISTRATIVO
8	MIGUEL ÁNGEL YÉPEZ MARTÍNEZ	Analista "G"	DIRECCIÓN DE DISEÑO, PLANEACIÓN Y SEGUIMIENTO DE POLÍTICAS PÚBLICAS EN PREVENCIÓN SOCIAL
9	ANA GABRIELA RAMOS PÉREZ	Analista "G"	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA EN LA PREVENCIÓN SOCIAL DE LA VIOLENCIA
10	JOSÉ IVÁN SANTIAGO LÓPEZ	Enlace "D"	ÁREA DE APOYO ADMINISTRATIVO
11	JUAN CARLOS CANCINO SÁNCHEZ	Enlace "D"	ÁREA DE APOYO ADMINISTRATIVO
12	BELEM CALVO ESTRADA	Enlace "D"	DIRECCIÓN DE DISEÑO, PLANEACIÓN Y SEGUIMIENTO DE POLÍTICAS PÚBLICAS EN PREVENCIÓN SOCIAL
13	JOSÉ CARLOS RUIZ MARTÍNEZ	Analista "G"	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA EN LA PREVENCIÓN SOCIAL DE LA VIOLENCIA
14	JORGE ARTURO CALDERÓN FIGUEROA	Analista "G"	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA EN LA PREVENCIÓN SOCIAL DE LA VIOLENCIA



**CENTRO ESTATAL DE PREVENCIÓN SOCIAL
DE LA VIOLENCIA Y PARTICIPACIÓN CIUDADANA**
Organismo Desconcentrado, jerárquicamente subordinado al Secretariado
Ejecutivo del Sistema Estatal de Seguridad Pública con plena autonomía administrativa

**CENTRO ESTATAL
DE PREVENCIÓN SOCIAL
DE LA VIOLENCIA
Y PARTICIPACIÓN CIUDADANA**

GOBIERNO DE CHIAPAS

15	KAREN ORDOÑEZ FLORES	Analista "G"	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA EN LA PREVENCIÓN SOCIAL DE LA VIOLENCIA
16	PERLA ROMINA PIÑÓN SÁNCHEZ	Analista "G"	DIRECCIÓN DE DISEÑO, PLANEACIÓN Y SEGUIMIENTO DE POLÍTICAS PÚBLICAS EN PREVENCIÓN SOCIAL
NO.	NOMBRE	CATEGORIA	ADSCRIPCIÓN
17	JUAN EMMANUEL MIRANDA ALBARRÁN	Analista "G"	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA EN LA PREVENCIÓN SOCIAL DE LA VIOLENCIA
18	AUREA MARTÍNEZ RUIZ	Analista "G"	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA EN LA PREVENCIÓN SOCIAL DE LA VIOLENCIA
19	VERÓNICA NATIVIDAD GARCIA BALLINAS	Analista "G"	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA EN LA PREVENCIÓN SOCIAL DE LA VIOLENCIA
20	JORGE ÁNGEL RAMÍREZ ZÚÑIGA	Analista "G"	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA EN LA PREVENCIÓN SOCIAL DE LA VIOLENCIA
21	OMAR SANTIAGO MONTERO	Analista "G"	ÁREA DE APOYO ADMINISTRATIVO
22	ARLETTE CASTILLO TRINIDAD	Analista "G"	ÁREA DE APOYO ADMINISTRATIVO
23	ROCIO JAQUELINE BARRIOS REYES	Analista "G"	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA EN LA PREVENCIÓN SOCIAL DE LA VIOLENCIA
24	FANNY RODRÍGUEZ GÓMEZ	Aux. Adtvo. "C"	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA EN LA PREVENCIÓN SOCIAL DE LA VIOLENCIA
25	JOSÉ ALEXANDER DOMÍNGUEZ ARÉVALO	Aux. Adtvo. "C"	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA EN LA PREVENCIÓN SOCIAL DE LA VIOLENCIA
26	ANABEL COELLO SANTIAGO	Aux. Adtvo. "C"	DIRECCIÓN DE DISEÑO, PLANEACIÓN Y SEGUIMIENTO DE POLÍTICAS PÚBLICAS EN PREVENCIÓN SOCIAL
27	ANDREA CAROLINA GONZÁLEZ GÓMEZ	Aux. Adtvo. "C"	DIRECCIÓN DE DISEÑO, PLANEACIÓN Y SEGUIMIENTO DE POLÍTICAS PÚBLICAS EN PREVENCIÓN SOCIAL



**CENTRO ESTATAL DE PREVENCIÓN SOCIAL
DE LA VIOLENCIA Y PARTICIPACIÓN CIUDADANA**
Organismo Desconcentrado, jerárquicamente subordinado al Secretariado
Ejecutivo del Sistema Estatal de Seguridad Pública con plena autonomía administrativa

CENTRO ESTATAL
DE PREVENCIÓN SOCIAL
DE LA VIOLENCIA
Y PARTICIPACIÓN CIUDADANA
GOBIERNO DE CHIAPAS

	MARTHA ALICIA MAZA LÓPEZ	Aux. Adtvo. "C"	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA EN LA PREVENCIÓN SOCIAL DE LA VIOLENCIA
29	MARÍA CANDELARIA JIMÉNEZ RODRÍGUEZ	Aux. Adtvo. "C"	DIRECCIÓN DE DISEÑO, PLANEACIÓN Y SEGUIMIENTO DE POLÍTICAS PÚBLICAS EN PREVENCIÓN SOCIAL
30	YURIDIA FAVIEL CERDA	Aux. Adtvo. "C"	DIRECCIÓN DE DISEÑO, PLANEACIÓN Y SEGUIMIENTO DE POLÍTICAS PÚBLICAS EN PREVENCIÓN SOCIAL
31	CARLOS DANIEL CRUZ MACÍAS	Aux. Adtvo. "C"	DIRECCIÓN DE DISEÑO, PLANEACIÓN Y SEGUIMIENTO DE POLÍTICAS PÚBLICAS EN PREVENCIÓN SOCIAL
32	LUCERO GUADALUPE LÓPEZ JONAPA	Aux. Adtvo. "C"	DIRECCIÓN DE DISEÑO, PLANEACIÓN Y SEGUIMIENTO DE POLÍTICAS PÚBLICAS EN PREVENCIÓN SOCIAL
NO.	NOMBRE	CATEGORIA	ADSCRIPCIÓN
33	MARÍA JOSÉ CÓRDOVA SOLÓRZANO	Aux. Adtvo. "C"	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA EN LA PREVENCIÓN SOCIAL DE LA VIOLENCIA
34	MARÍA CONCEPCIÓN CRUZ LÓPEZ	Aux. Adtvo. "C"	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA EN LA PREVENCIÓN SOCIAL DE LA VIOLENCIA
35	OLGA PATRICIA HERNÁNDEZ CHÁVEZ	Aux. Adtvo. "C"	DIRECCIÓN DE DISEÑO, PLANEACIÓN Y SEGUIMIENTO DE POLÍTICAS PÚBLICAS EN PREVENCIÓN SOCIAL
36	YESENIA GUADALUPE LÓPEZ CRUZ	Aux. Adtvo. "C"	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA EN LA PREVENCIÓN SOCIAL DE LA VIOLENCIA
37	MARÍA GUADALUPE HERRERA PÉREZ	Auxiliar Administrativo "B"	DIRECCIÓN GENERAL
38	MARÍA EUGENIA SANTIAGO CARPIO	Enlace A	DIRECCIÓN GENERAL
39	VLADIMIR AGUILAR GÓMEZ	Analista "G"	ÁREA DE APOYO ADMINISTRATIVO
40	JAIME GÓMEZ SANTIZ	Analista "G"	ÁREA DE APOYO ADMINISTRATIVO



**CENTRO ESTATAL DE PREVENCIÓN SOCIAL
DE LA VIOLENCIA Y PARTICIPACIÓN CIUDADANA**
Organismo Desconcentrado, jerárquicamente subordinado al Secretariado
Ejecutivo del Sistema Estatal de Seguridad Pública con plena autonomía administrativa

**CENTRO ESTATAL
DE PREVENCIÓN SOCIAL
DE LA VIOLENCIA
Y PARTICIPACIÓN CIUDADANA**
GOBIERNO DE CHIAPAS

41	EDITH BECK CANO	Analista "G"	ÁREA DE APOYO ADMINISTRATIVO
42	JULIO CÉSAR BERMÚDEZ MAZARIEGOS	Mando Medio "E"	DIRECCIÓN DE DISEÑO, PLANEACIÓN Y SEGUIMIENTO DE POLÍTICAS PÚBLICAS EN PREVENCIÓN SOCIAL
43	HARRY WILLIAMS LÓPEZ ZOMA	Analista "G"	DIRECCIÓN DE DISEÑO, PLANEACIÓN Y SEGUIMIENTO DE POLÍTICAS PÚBLICAS EN PREVENCIÓN SOCIAL
44	GUADALUPE IVONNE LEAL VÁZQUEZ	Analista "G"	DIRECCIÓN DE DISEÑO, PLANEACIÓN Y SEGUIMIENTO DE POLÍTICAS PÚBLICAS EN PREVENCIÓN SOCIAL
45	GABRIELA ALEJANDRA SOLÍS TOLEDO	Mando Medio "E"	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA EN LA PREVENCIÓN SOCIAL DE LA VIOLENCIA
46	YESSICA GUADALUPE NAVARRO ESPINOSA	Analista "G"	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA EN LA PREVENCIÓN SOCIAL DE LA VIOLENCIA
47	MARLEN DEL ROSARIO ARRÓNIZ GÓMEZ	DIRECTORA GENERAL	DIRECCIÓN GENERAL
48	SUSANA ALEJANDRA CAMACHO LÓPEZ	JEFA DE ÁREA	ÁREA DE APOYO ADMINISTRATIVO

La unidad administrativa que observa mayor estado de vulnerabilidad y riesgo de los datos personales es el Área de Apoyo Administrativo con 1.5 de riesgo, seguida en orden descendente por la Dirección de Participación Ciudadana en la Prevención Social de la Violencia con 1.25 de riesgo, la Dirección de Diseño, Planeación y Seguimiento de Políticas Públicas en Prevención Social con 1.0 de riesgo, y la Dirección General con 0.75 de riesgo.

Al respecto, hay que señalar además que la etapa del ciclo de vida (obtención, tratamiento, almacenamiento, transferencia, bloqueo y eliminación) en la que los datos personales se encuentran más vulnerables, es en el periodo de almacenamiento en un 30%; mientras que el periodo que implica menor riesgo es el de bloqueo con un 1%.

Las amenazas a las que se ven expuestos son básicamente:

- Robo, extravío o copia no autorizada.
- Uso, acceso o tratamiento no autorizado.



- Daño, alteración o modificación no autorizada.
- Pérdida o destrucción no autorizada.

Siendo la más alta, la de robo, extravío o copia no autorizada y la de menor riesgo es daño, alteración o modificación no autorizada.

Finalmente, como parte del análisis es posible establecer que el nivel de riesgo es mayormente medio, debido que se trabaja sobre todo con datos de identificación, en algunos casos con datos patrimoniales y son en un tratamiento se solicita un dato sensible. Asimismo, los datos personales corresponden a menos de 1000 personas, lo que reduce el nivel de riesgo y se mantienen a resguardo en computadoras personales con contraseña y en archiveros con llave para ampliar el margen de seguridad.

PROGRAMA DE TRABAJO PARA LA IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD

Conforme al análisis de brecha, existen algunas medidas de seguridad que se requiere implementar, por lo que a continuación se presentan las actividades generales que se planea realizar:

- Celebración de reuniones de trabajo con unidades administrativas a efecto de identificar alternativas de solución técnicas, físicas y administrativas a desarrollar en el mediano y largo plazo.
- Promover un sistema de gestión y administración de datos personales que permita centralizar mediante la identificación de datos por categorías, asociando los diversos tratamientos y procesos a las políticas de seguridad que resultan aplicables a cada caso, conforme a los estándares y mejores prácticas en la materia.
- Implementar mecanismos de divulgación y conocimiento de las políticas generales de seguridad y, verificar de manera continua su cumplimiento.
- Fortalecer los mecanismos de control de documentos e información en las distintas unidades administrativas, a efecto de evitar posibles vulneraciones.

Medidas de seguridad generales

Las medidas generales de seguridad administrativas, físicas y técnicas con las que actualmente cuenta el CEPVPC para



mantener la confidencialidad e integralidad de la información, así como para proteger los datos personales contra daño, pérdida, destrucción o alteración, así como evitar el uso, acceso o tratamiento no autorizado, e impedir la divulgación no autorizada, son las siguientes:

A) Medidas administrativas

1. Diseño y desarrollo de un modelo de capacitación permanente en materia de la Ley de Protección de Datos Personales en posesión de Sujetos Obligados del Estado de Chiapas (LPDPPSOCHIS), impartido a quienes colaboran en el CEPSVyPC.
2. Implementación de formatos de entrada y salida de préstamo de documentos por parte del área encargada del archivo.
3. Resguardo de los expedientes bajo los criterios, directrices y lineamientos para la atención de los expedientes técnicos.
4. Mecanismos de control desarrollados conforme a lo establecido en los lineamientos del Sistema de Gestión de Documentos institucional.
5. Suscripción de una carta responsiva por parte de los usuarios o personal con acceso a sistemas de datos personales, acerca del deber de confidencialidad.
6. Reportar al superior jerárquico los incidentes detectados respecto de pérdida o alteración de cualquier documento que contengan datos personales.

B) Medidas físicas

1. Resguardo de documentos e información en archivos físicos de trámite y concentración.
2. Disponer de la instalación de chapas con llave para mantener control de acceso de personas a espacios de resguardo de información.
3. Limitar el número de personas con acceso a archivos físicos.
4. Realizar el registro de personas con acceso a espacios físicos en los que se resguarda información con datos personales.
5. Procurar suscribir responsivas de confidencialidad con el personal que trata datos personales.
6. Designación de personal con acceso controlado a espacios de resguardo físico de expedientes y documentos con datos personales.

7. Resguardo de llaves en oficinas de acceso restringido.

C) Medidas técnicas

1. Utilizar claves de usuario y contraseñas de manera personal, y evitar compartirlas, prestarlas o registrarlas a la vista de otras personas.
2. Establecer y utilizar contraseñas robustas, es decir, de al menos ocho caracteres alfanuméricos y especiales, evitando que sean iguales al nombre del usuario, o cualquier otro nombre de personas, considerando que éstas sean fáciles de recordar y difíciles de adivinar o descifrar por un tercero, a fin de salvaguardar la información y datos personales a los que se tenga acceso.
3. Notificar de manera inmediata al Área de Apoyo Administrativo los casos en los que los usuarios identifiquen o consideren que sus claves de usuario y/o contraseñas han sido utilizadas por un tercero, para las prevenciones conducentes.
4. Procurar la utilización de una cuenta de correo electrónico oficial para fines relacionados con las actividades laborales, evitando remitir datos personales.
5. Mantener los documentos electrónicos y físicos en lugares seguros, bajo llave, dentro de cajones cerrados, o bajo la protección de alguna contraseña, a fin de promover la restricción a los datos personales que pudieran contener.
6. No difundir, transmitir o compartir documentos electrónicos ni físicos que contengan datos personales, a fin de garantizar que estos no sean divulgados de manera no autorizada.
7. Evitar dejar u olvidar los documentos físicos que contengan datos personales en los equipos de impresión, así como evitar su impresión, escaneo y fotocopiado si no es realmente requerido para las actividades laborales.
8. Evitar el acceso a los sistemas de información de tratamiento de datos personales, bajo el precepto del mínimo privilegio; es decir, únicamente al personal que por sus funciones y facultades laborales los requiera, a fin de mantener una adecuada segregación de funciones, restricción de acceso y tratamiento de esos datos.
9. Borrar o eliminar de la papelería de reciclaje del escritorio de los equipos de



cómputo los documentos o archivos electrónicos que nos son necesarios para el desarrollo de funciones.

10. Notificar las bajas de accesos a los sistemas de información o de tratamiento de datos personales, con oportunidad, para restringir el acceso a dichos datos por personal no autorizado.

Adicionalmente, como parte de la política de seguridad técnica, el Área de Apoyo Administrativo implementa los siguientes controles:

1. Definición de políticas de contraseñas.
2. Asignación privilegios de acuerdo a roles y funciones.
3. Agente de seguridad instalado en administrativos de servidores de correo electrónico.
4. Tareas de respaldo por servidor y por agente.
5. Autenticación de correo electrónico.
6. Operación Hardening (proceso de asegurar un sistema reduciendo sus vulnerabilidades o agujeros de seguridad, para los que se está más propenso cuanto más funciones desempeña, sistema con una única función es más seguro que uno con muchos propósitos, proceso de cerrar las vías para los ataques más típicos incluye el cambio de claves por defecto, desinstalar el software y dar de baja usuarios y accesos innecesarios, también deshabilitar servicios que no serán usados y fortalecer las configuraciones de aquellos que estarán en uso), en los servidores de Información en alta disponibilidad con contraseña de directorio de datos y acceso restringido.
7. Tareas de respaldo por servidor y de las instancias de base de datos del servicio.
8. Acceso a los sistemas conforme al procedimiento de administración de usuarios y contraseñas con cuenta local con permiso de administrador.
9. Borrado seguro de la información que reside en los equipos de cómputo.
10. Deshabilitación de cuentas de personal que causa baja.
11. Acceso controlado de administración y accesos privilegiados.
12. Definición de procedimientos y controles de seguridad de la información.



CHIAPAS
GOBIERNO DEL ESTADO

Monitoreo de las medidas de seguridad

Como parte del programa de protección de datos personales, es importante la supervisión de las medidas de seguridad técnicas y físicas, como un elemento para la mejora continua, que permite definir nuevas formas de monitoreo, de acuerdo con las necesidades surgidas al interior del CEPsVyPC, entre las que podemos señalar las siguientes:

1. Revisión y actualización permanente de las contraseñas utilizadas para resguardar los datos personales en equipos de cómputo.
2. Monitorear que todas las cuentas que se dan de alta para otorgar acceso a la red, sea validada en el campo correspondiente a la contraseña, a fin de asegurar el uso.
3. Revisar el cumplimiento de protocolos.
4. Validar que los accesos, baja o cambio a sistemas se realicen conforme al proceso de administración de usuarios.
5. Vigilar que el ingreso de personas sea a través de los accesos correspondientes, plenamente identificados.

PROPUESTA DE CAPACITACIÓN EN MATERIA DE DATOS PERSONALES

Uno de los factores esenciales para la implementación de los controles y demás medidas de seguridad, la actualización y mejora continua del inventario de datos personales, el apego a la normatividad y a Ley, así como la concientización en la materia por parte del personal involucrado en el tratamiento de datos personales, es el conocimiento y capacitación, por lo que el aprovechamiento de los recursos y herramientas que el propio Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) ha dispuesto para su uso y obtención de beneficios, se propone que a través del Centro Estatal de Prevención Social de la Violencia y Participación Ciudadana, en coordinación con la Dirección de Capacitación y Promoción de la Transparencia del Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Chiapas, se desarrolle un programa de capacitación focalizada, mediante el cual profundice en el conocimiento de la materia por parte de los servidores públicos que intervienen en el tratamiento de datos personales.



Así, entre los elementos de los que resulta necesario profundizar se encuentran los siguientes:

I) Obligaciones en la observancia de la LPDPPSOCHIS

- ✓ Principios
- ✓ Deberes
- ✓ Sistemas de datos personales
- ✓ Medidas de seguridad
- ✓ Procedimientos y sanciones/ Derechos ARCO (acceso, rectificación, cancelación y oposición)
- ✓ Medios de defensa

II) La Ley de protección de datos personales en posesión de sujetos obligados en Chiapas y la LGPDPPSO y sus Lineamientos

- ✓ Antecedentes
- ✓ Principios.
- ✓ Alcances
- ✓ Objetivo
- ✓ Implicaciones

III) El programa de protección de datos personales

- ✓ Sistemas de datos personales
- ✓ Inventario y Base de Datos
- ✓ Medidas de seguridad
- ✓ Análisis de brecha y de riesgo
- ✓ Funciones y obligaciones

IV) El principio de información: Avisos de Privacidad en el marco del programa de protección de datos personales

- ✓ Contenido: Integral, simplificado



**CENTRO ESTATAL DE PREVENCIÓN SOCIAL
DE LA VIOLENCIA Y PARTICIPACIÓN CIUDADANA**
Organismo Desconcentrado, jerárquicamente subordinado al Secretariado
Ejecutivo del Sistema Estatal de Seguridad Pública con plena autonomía administrativa

CENTRO ESTATAL
DE PREVENCIÓN SOCIAL
DE LA VIOLENCIA
Y PARTICIPACIÓN CIUDADANA
GOBIERNO DE CHIAPAS

- ✓ Consentimiento
- ✓ Deber de información
- ✓ Finalidades del tratamiento de los datos

NO.	NOMBRE	CATEGORIA	ADSCRIPCIÓN
1	OMAR SANTIAGO CHAMPO	Enlace “D”	ÁREA DE APOYO ADMINISTRATIVO
2	VICTOR MANUEL CHACÓN ROJAS	Enlace “D”	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA EN LA PREVENCIÓN SOCIAL DE LA VIOLENCIA
3	FABIÁN HERNÁNDEZ CONSOSPO	Enlace “D”	ÁREA DE APOYO ADMINISTRATIVO
4	GABRIELA GUADALUPE PÉREZ HUERTA	Enlace “D”	DIRECCIÓN DE DISEÑO, PLANEACIÓN Y SEGUIMIENTO DE POLÍTICAS PÚBLICAS EN PREVENCIÓN SOCIAL
5	JESSICA ALEJANDRA SARMIENTO GALLEGOS	Enlace “D”	DIRECCIÓN DE DISEÑO, PLANEACIÓN Y SEGUIMIENTO DE POLÍTICAS PÚBLICAS EN PREVENCIÓN SOCIAL
6	SILKE PAMELA ZAMORA LÓPEZ	Enlace “D”	DIRECCIÓN DE DISEÑO, PLANEACIÓN Y SEGUIMIENTO DE POLÍTICAS PÚBLICAS EN PREVENCIÓN SOCIAL
7	ROGER GONZÁLEZ CHÁVEZ	Enlace “D”	ÁREA DE APOYO ADMINISTRATIVO
8	MIGUEL ÁNGEL YÉPEZ MARTÍNEZ	Analista “G”	DIRECCIÓN DE DISEÑO, PLANEACIÓN Y SEGUIMIENTO DE POLÍTICAS PÚBLICAS EN PREVENCIÓN SOCIAL
9	ANA GABRIELA RAMOS PÉREZ	Analista “G”	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA EN LA PREVENCIÓN SOCIAL DE LA VIOLENCIA
10	JOSÉ IVÁN SANTIAGO LÓPEZ	Enlace “D”	ÁREA DE APOYO ADMINISTRATIVO
11	JUAN CARLOS CANCINO SÁNCHEZ	Enlace “D”	ÁREA DE APOYO ADMINISTRATIVO
12	BELEM CALVO ESTRADA	Enlace “D”	DIRECCIÓN DE DISEÑO, PLANEACIÓN Y SEGUIMIENTO DE POLÍTICAS PÚBLICAS EN PREVENCIÓN SOCIAL
13	JOSÉ CARLOS RUIZ MARTÍNEZ	Analista “G”	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA EN LA PREVENCIÓN SOCIAL DE LA VIOLENCIA
14	JORGE ARTURO CALDERÓN FIGUEROA	Analista “G”	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA EN LA PREVENCIÓN SOCIAL DE LA VIOLENCIA
15	KAREN ORDOÑEZ FLORES	Analista “G”	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA EN LA PREVENCIÓN SOCIAL DE LA VIOLENCIA
16	PERLA ROMINA PIÑÓN SÁNCHEZ	Analista “G”	DIRECCIÓN DE DISEÑO, PLANEACIÓN Y SEGUIMIENTO DE POLÍTICAS PÚBLICAS EN PREVENCIÓN SOCIAL

“Los datos personales recabados en este formato, serán protegidos, incorporados y tratados en los términos establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en los Lineamientos Generales para la Custodia y Protección de Datos Personales e Información Reservada y Confidencial en Posesión de los Sujetos Obligados del Estado de Chiapas y demás Normatividad aplicable”.

“La información de este documento, así como la contenida en los documentos que se adjuntan, puede ser objeto de solicitudes de acceso a la información pública, así mismo puede contener información confidencial o legalmente protegida y está destinado únicamente para el uso del destinatario (s) previsto. Cualquier divulgación, difusión, distribución, copia o la toma de cualquier acción basada en la información aquí contenida está prohibido”

NO.	NOMBRE	CATEGORIA	ADSCRIPCIÓN
17	JUAN EMMANUEL MIRANDA ALBARRÁN	Analista “G”	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA EN LA PREVENCIÓN SOCIAL DE LA VIOLENCIA
18	AUREA MARTÍNEZ RUIZ	Analista “G”	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA EN LA PREVENCIÓN SOCIAL DE LA VIOLENCIA
19	VERÓNICA NATIVIDAD GARCIA BALLINAS	Analista “G”	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA EN LA PREVENCIÓN SOCIAL DE LA VIOLENCIA
20	JORGE ÁNGEL RAMÍREZ ZUÑIGA	Analista “G”	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA EN LA PREVENCIÓN SOCIAL DE LA VIOLENCIA
21	OMAR SANTIAGO MONTERO	Analista “G”	ÁREA DE APOYO ADMINISTRATIVO
22	ARLETTE CASTILLO TRINIDAD	Analista “G”	ÁREA DE APOYO ADMINISTRATIVO
23	ROCIO JAQUELINE BARRIOS REYES	Analista “G”	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA EN LA PREVENCIÓN SOCIAL DE LA VIOLENCIA
24	FANNY RODRÍGUEZ GÓMEZ	Aux. Adtvo. “C”	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA EN LA PREVENCIÓN SOCIAL DE LA VIOLENCIA
25	JOSÉ ALEXANDER DOMÍNGUEZ ARÉVALO	Aux. Adtvo. “C”	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA EN LA PREVENCIÓN SOCIAL DE LA VIOLENCIA
26	ANABEL COELLO SANTIAGO	Aux. Adtvo. “C”	DIRECCIÓN DE DISEÑO, PLANEACIÓN Y SEGUIMIENTO DE POLÍTICAS PÚBLICAS EN PREVENCIÓN SOCIAL
27	ANDREA CAROLINA GONZÁLEZ GÓMEZ	Aux. Adtvo. “C”	DIRECCIÓN DE DISEÑO, PLANEACIÓN Y SEGUIMIENTO DE POLÍTICAS PÚBLICAS EN PREVENCIÓN SOCIAL
28	MARTHA ALICIA MAZA LÓPEZ	Aux. Adtvo. “C”	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA EN LA PREVENCIÓN SOCIAL DE LA VIOLENCIA
29	MARÍA CANDELARIA JIMÉNEZ RODRÍGUEZ	Aux. Adtvo. “C”	DIRECCIÓN DE DISEÑO, PLANEACIÓN Y SEGUIMIENTO DE POLÍTICAS PÚBLICAS EN PREVENCIÓN SOCIAL
30	YURIDIA FAVIEL CERDA	Aux. Adtvo. “C”	DIRECCIÓN DE DISEÑO, PLANEACIÓN Y SEGUIMIENTO DE POLÍTICAS PÚBLICAS EN PREVENCIÓN SOCIAL
31	CARLOS DANIEL CRUZ MACÍAS	Aux. Adtvo. “C”	DIRECCIÓN DE DISEÑO, PLANEACIÓN Y SEGUIMIENTO DE POLÍTICAS PÚBLICAS EN PREVENCIÓN SOCIAL
32	LUCERO GUADALUPE LÓPEZ JONAPA	Aux. Adtvo. “C”	DIRECCIÓN DE DISEÑO, PLANEACIÓN Y SEGUIMIENTO DE POLÍTICAS PÚBLICAS EN PREVENCIÓN SOCIAL

“Los datos personales recabados en este formato, serán protegidos, incorporados y tratados en los términos establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en los Lineamientos Generales para la Custodia y Protección de Datos Personales e Información Reservada y Confidencial en Posesión de los Sujetos Obligados del Estado de Chiapas y demás Normatividad aplicable”.

“La información de este documento, así como la contenida en los documentos que se adjuntan, puede ser objeto de solicitudes de acceso a la información pública, así mismo puede contener información confidencial o legalmente protegida y está destinado únicamente para el uso del destinatario (s) previsto. Cualquier divulgación, difusión, distribución, copia o la toma de cualquier acción basada en la información aquí contenida está prohibido”

NO.	NOMBRE	CATEGORIA	ADSCRIPCIÓN
33	MARÍA JOSÉ CÓRDOVA SOLÓRZANO	Aux. Adtvo. “C”	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA EN LA PREVENCIÓN SOCIAL DE LA VIOLENCIA
34	MARÍA CONCEPCIÓN CRUZ LÓPEZ	Aux. Adtvo. “C”	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA EN LA PREVENCIÓN SOCIAL DE LA VIOLENCIA
35	OLGA PATRICIA HERNÁNDEZ CHÁVEZ	Aux. Adtvo. “C”	DIRECCIÓN DE DISEÑO, PLANEACIÓN Y SEGUIMIENTO DE POLÍTICAS PÚBLICAS EN PREVENCIÓN SOCIAL
36	YESENIA GUADALUPE LÓPEZ CRUZ	Aux. Adtvo. “C”	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA EN LA PREVENCIÓN SOCIAL DE LA VIOLENCIA
37	MARÍA GUADALUPE HERRERA PÉREZ	Auxiliar Administrativo “B”	DIRECCIÓN GENERAL
38	MARÍA EUGENIA SANTIAGO CARPIO	Enlace A	DIRECCIÓN GENERAL
39	VLADIMIR AGUILAR GÓMEZ	Analista “G”	ÁREA DE APOYO ADMINISTRATIVO
40	JAIME GÓMEZ SANTIZ	Analista “G”	ÁREA DE APOYO ADMINISTRATIVO
41	EDITH BECK CANO	Analista “G”	ÁREA DE APOYO ADMINISTRATIVO
42	JULIO CÉSAR BERMÚDEZ MAZARIEGOS	Mando Medio “E”	DIRECCIÓN DE DISEÑO, PLANEACIÓN Y SEGUIMIENTO DE POLÍTICAS PÚBLICAS EN PREVENCIÓN SOCIAL
43	HARRY WILLIAMS LÓPEZ ZOMA	Analista “G”	DIRECCIÓN DE DISEÑO, PLANEACIÓN Y SEGUIMIENTO DE POLÍTICAS PÚBLICAS EN PREVENCIÓN SOCIAL
44	GUADALUPE IVONNE LEAL VÁZQUEZ	Analista “G”	DIRECCIÓN DE DISEÑO, PLANEACIÓN Y SEGUIMIENTO DE POLÍTICAS PÚBLICAS EN PREVENCIÓN SOCIAL
45	GABRIELA ALEJANDRA SOLÍS TOLEDO	Mando Medio “E”	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA EN LA PREVENCIÓN SOCIAL DE LA VIOLENCIA
46	YESSICA GUADALUPE NAVARRO ESPINOSA	Analista “G”	DIRECCIÓN DE PARTICIPACIÓN CIUDADANA EN LA PREVENCIÓN SOCIAL DE LA VIOLENCIA
47	MARLEN DEL ROSARIO ARRÓNIZ GÓMEZ	DIRECTORA GENERAL	DIRECCIÓN GENERAL
48	SUSANA ALEJANDRA CAMACHO LÓPEZ	JEFA DE ÁREA	ÁREA DE APOYO ADMINISTRATIVO

"2024, Año de Felipe Carrillo Puerto, Benemérito del Proletariado, Revolucionario y Defensor del Mayab"

**EDITH BECK CANO
P R E S E N T E**

Con fundamento en lo dispuesto por el artículo 5º del Decreto de Creación por el que se crea el Centro Estatal de Prevención Social de la Violencia y Participación Ciudadana, así como los artículos 7 fracción I inciso A y 14 fracciones VI y X de su Reglamento Interior, tengo a bien ratificarle:

**OFICIAL DE PROTECCIÓN DE DATOS PERSONALES ANTE EL
INSTITUTO DE TRANSPARENCIA, ACCESO A LA
INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES
DEL ESTADO DE CHIAPAS. (ITAIPCH)**

Con las prerrogativas, derechos, y obligaciones que confiere a dicho cargo la Legislación Estatal, exhortándolo a cumplir sus actividades y encomiendas bajo los principios de Legalidad, Honradez, Lealtad, Imparcialidad y Eficiencia.

**"POR EL CENTRO ESTATAL DE PREVENCIÓN SOCIAL DE LA
VIOLENCIA Y PARTICIPACIÓN CIUDADANA"**



**MARLEN DEL ROSARIO ARRÓNIZ GÓMEZ
ENCARGADA DE LA DIRECCIÓN GENERAL**

TUXTLA GUTIÉRREZ, CHIAPAS; A 08 DE FEBRERO DE 2024

Seguidores de Facebook



Publicación de Facebook de fecha 03 de octubre de 2024.

Centro Estatal de Prevención Social de la Violencia Chiapas
3 de octubre a las 3:46 pm · 🌐 · 📍

#protecciondedatospersonales #CESPVyPC



¿Sabías que...?

La nube tiene las siguientes ventajas:

- Disponibilidad de la información a toda hora y en cualquier lugar.
- Realizar copias de seguridad de la información.
- Compartir información con quien decidas.
- Acceso a tu información con cualquier dispositivo móvil.

En un mundo cada vez más digital, hay muchas maneras en las que los datos podrían estar en peligro, pero algunos de los riesgos de seguridad en la nube más comunes provienen de:

- Fraudes electrónicos.
- Contraseñas débiles.
- Vulnerabilidad de las aplicaciones.
- Un Infiltrado.
- Errores de los usuarios.

¡No pongas en peligro tu información!

"Para conocer más sobre este tema, visita el Micrositio de Ciberseguridad del Instituto Federal de Telecomunicaciones y consulta las Recomendaciones para mantener segura tu privacidad y datos personales en el entorno digital del INAI."

EN EL USO DE LAS TECNOLOGÍAS, INFORMARSE ES PROTEGERTE.

#SoyUsuarioLosDatosPersonalesEnLaNube #UnidosPorLaSeguridadDigital

WWW.IFT.ORG.MX
IFT Twitter, IFT YouTube, Facebook, Instagram, LinkedIn

WWW.INAI.ORG.MX
INAI Twitter, INAI Facebook, INAI Instagram, INAI LinkedIn

Publicación de Facebook de fecha 10 de octubre de 2024.

Centro Estatal de Prevención Social de la Violencia Chiapas
10 de octubre a las 3:40 pm · 🌐 · 📍

#protecciondedatospersonales #CESPVyPC



La sombra digital, ¿qué es?

Una sombra digital es el rastro de datos que dejas cuando usas Internet. Esto incluye los sitios web que visitas, los correos electrónicos que envías y la información que compartes online.

¿De qué manera dejamos sombras digitales?

- Compras online
- Operaciones bancarias online
- Redes sociales
- Consulta de sitios web

El IFT y el INAI te recomendamos que...

Al utilizar algún navegador, lo hagas de manera incógnita, en caso de acceder con tu cuenta, es importante que borres los datos de navegación, el historial de descargas, cookies, contraseña y datos almacenados.

De igual forma, se sugiere evitar el uso de computadoras públicas o conectarte a una red pública cuando accedas a tu información personal o realices operaciones de banca en línea.

Para conocer más sobre este tema, visita el **Micrositio de Ciberseguridad** del Instituto Federal de Telecomunicaciones y consulta las **Recomendaciones para mantener segura tu privacidad y datos personales en el entorno digital del INAI.**

EN EL USO DE LAS TECNOLOGÍAS, INFORMARSE ES PROTEGERTE.

#SoyUsuario#SombraDigital#UnidosPorLaSeguridadDigital

WWW.IFT.ORG.MX
IFT Twitter, IFT YouTube, Facebook, Instagram, LinkedIn

WWW.INAI.ORG.MX
INAI Twitter, INAI Facebook, INAI Instagram, INAI LinkedIn



Centro Estatal de Prevención Social de la Violencia Chiapas

17 de octubre a las 3:26 pm

#ProtecciónDeDatosPersonales

#CESPVyPC



Centro Estatal de Prevención Social de la Violencia Chiapas

Protección de Datos Personales



- Aceptar sólo a personas conocidas:**

Evitar aceptar todas las solicitudes de contacto de forma compulsiva e investigar quién es la persona que solicita el contacto.
- Evitar publicar información de contacto físico:**

Evitar publicar información que permita conocer dónde vive, trabaja o estudia, o a los lugares de ocio que frecuenta.
- Cuidar la publicación de ubicaciones:**

Las personas usuarias deben tener especial cuidado respecto a la publicación de información relativa a los lugares en que se encuentran.
- Usar diferentes nombres de usuario y usuario y contraseñas robustas:**

Es recomendable emplear diferentes nombres y contraseñas robustas para entrar en las distintas redes sociales.
- Utilizar contraseñas seguras:**

Se recomienda que tengan una extensión mínima de 8 caracteres, ser alfanuméricas, utilizar letras mayúsculas y minúsculas, así como caracteres especiales.

INAI México

IFT_MX f IFT_mx @iftmexico Y IFTMX



Centro Estatal de Prevención Social de la Violencia Chiapas

23 de octubre a las 3:30pm



INAI

#protecciondedatospersonales #CESPVyPC



IFT



Centro Estatal de Prevención Social de la Violencia Chiapas



INAI

MANTÉN TUS DATOS PROTEGIDOS DURANTE EL USO DE LA IA

Los sistemas de IA suelen depender de grandes bases de información que incluyen datos personales compilados, intercambiados, combinados y analizados con diversos métodos que en ocasiones suelen ser opacos¹. Por ello, el INAI y el IFT te presentan las siguientes recomendaciones:

1. Infórmate sobre los avisos de privacidad y/o las políticas de privacidad antes de usar servicios de IA.
2. Mantén dispositivos y aplicaciones actualizados.
3. Limita el acceso de la IA ajustando las configuraciones de privacidad.
4. Elige servicios de IA de proveedores confiables que cumplan con los estándares de seguridad y protección de datos personales.
5. Evita proporcionar información que comprometa tus datos personales, como nombres, direcciones, números de teléfono o información bancaria.
6. Comparte sólo la información necesaria para obtener una respuesta o asistencia.

Recuerda la importancia de equilibrar la innovación con la protección de los datos personales en el camino hacia un entorno digital más seguro.

Para conocer más sobre este tema, visita el [Manifiesto de Ciberseguridad del IFT](#) y las [Recomendaciones para el tratamiento de datos personales](#) derivado del uso de la Inteligencia Artificial del INAI.

EN EL USO DE LAS TECNOLOGÍAS, INFORMARTE ES PROTEGERTE

#SoyUsuario #DatosPersonales #UnidosPorLaSeguridadDigital

1. GARY O'NEILL, EL ALTO COMISIONADO DE LAS NACIONES UNIDAS PARA LOS DERECHOS HUMANOS, LAS reglas de la inteligencia artificial para la privacidad exigen mantener opacos: @charlie. Dependiendo de qué datos están siendo recopilados y cómo se configuran, más privacidad digital, menos privacidad.

WWW.IFT.ORG.MX







WWW.INAI.ORG.MX







Publicación de Facebook de fecha 29 de octubre de 2024.

 Centro Estatal de Prevención Social de la Violencia Chiapas
Hoy a las 3:14 pm · 🌐 · 🌐

#protecciondedatospersonales
#CESPVyPC

RECOMENDACIONES EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES DIRIGIDAS A CENTROS EDUCATIVOS

¡CAPACÍTATE!

En la página del INAI tenemos diferentes documentos que pueden ayudarte a capacitar sobre diferentes temas, tales como:

Conceptos clave: Aborda los fundamentos de la protección de datos personales.

- ✕ **Principios y deberes:** Explica los principios y deberes reconocidos por la legislación en materia de protección de datos personales.
- ✕ **Recepción de datos personales:** Importancia del tratamiento de datos.
- ✕ **Avisos de privacidad:** Explica con detalle lo que debe contener un aviso de privacidad.
- ✕ **Documento de seguridad:** Información sobre la importancia de elaborar un documento que describa las medidas de seguridad adoptadas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.



Seguidores de X

Centro Estatal de Prevención Social Chiapas
3,191 posts

Siguiendo

Centro Estatal de Prevención Social Chiapas
@prevenchiapas

Blvd. Belisario Domínguez 1713 Planta Baja, Xamaipak C.P. 29067 Tuxtla Gutiérrez, Chiapas [#CEPSVyPC](#) [#ChiapasDeCorazón](#)

Chiapas, México prevencion.chiapas.gob.mx

Se unió en octubre de 2013

320 Siguiendo **1.626** Seguidores

Ninguna de las cuentas que sigues sigue a este usuario

Publicación de X de fecha 29 de octubre de 2024.

 **Centro Estatal de Prevención Social Chiapas** @prevenchiapas · 11s
#protecciondeDatosPersonales
#CESPVyPC

 **¿Sabías que...?**  

La nube tiene las siguientes ventajas:

- Disponibilidad de la información a toda hora y en cualquier lugar.
- Realizar copias de seguridad de la información.
- Compartir información con quien decidas.
- Acceso a tu información con cualquier dispositivo móvil.

En un mundo cada vez más digital, hay muchas maneras en las que los datos podrían estar en peligro, pero algunos de los riesgos de seguridad en la nube más comunes provienen de:

- Fraudes electrónicos.
- Contraseñas débiles.
- Vulnerabilidad de las aplicaciones.
- Un infiltrado.
- Errores de los usuarios.

¡No pongas en peligro tu información!

"Para conocer más sobre este tema, visita el Micrositio de Ciberseguridad del Instituto Federal de Telecomunicaciones y consulta las Recomendaciones para mantener segura tu privacidad y datos personales en el entorno digital del INAI."

EN EL USO DE LAS TECNOLOGÍAS, INFORMARSE ES PROTEGERSE.

**#SoyUsuario#LosDatosPersonalesEnLaNube
#UnidosPorLaSeguridadDigital**

WWW.IFT.ORG.MX


WWW.INAI.ORG.MX


Vulneraciones a los Sistemas de Información y Bases de Datos

CONTENIDO DE LA BÍTACORA	COMPLETE EL CONTENIDO DE LA BÍTACORA
FECHA DEL INCIDENTE:	
NOMBRE:	
CARGO:	
DIRECCIÓN O ÁREA:	
RESPONSABLE DEL ÁREA:	
CAUSA DE LA VULNERACIÓN:	
SISTEMA(S) DE INFORMACIÓN O BASE(S) DE DATO(S) VULNERADO(S)	
ACCIONES CORRECTIVAS IMPLEMENTADAS DE MANERA INMEDIATA Y DEFINITIVA	
CANTIDAD DE TITULARES	
SOPORTE DE LA INFORMACIÓN VULNERADA	<input type="checkbox"/> Físico <input type="checkbox"/> Electrónico <input type="checkbox"/> Mixto
SELECCIONE EL TIPO DE VULNERACIÓN	<input type="checkbox"/> Pérdida o destrucción no autorizada <input type="checkbox"/> Robo, extravío o copia no autorizada <input type="checkbox"/> Uso, acceso o tratamiento no autorizado <input type="checkbox"/> Daño, alteración o modificación no autorizada
TIPO DE DATOS PERSONALES COMPROMETIDOS	<input type="checkbox"/> Identificativos <input type="checkbox"/> Laborales <input type="checkbox"/> Tránsito y Movimientos Migratorios <input type="checkbox"/> Académicos <input type="checkbox"/> Procedimientos Administrativos o Judiciales <input type="checkbox"/> Patrimonial <input type="checkbox"/> Salud <input type="checkbox"/> Ideológicos <input type="checkbox"/> De origen <input type="checkbox"/> Características Personales <input type="checkbox"/> Vida Sexual <input type="checkbox"/> Religiosos
Nombre y firma del titular de la dirección o área	Nombre y firma del titular de datos personales
	Nombre y firma del titular del ITAIPCH

Los datos personales recabados en este formato, serán protegidos, incorporados y tratados en los términos establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en los Lineamientos Generales para la Custodia y Protección de Datos Personales e Información Reservada y Confidencial en Posesión de los Sujetos Obligados del Estado de Chiapas y demás Normatividad aplicable.

La información de este documento, así como la contenida en los documentos que se adjuntan, puede ser objeto de solicitudes de acceso a la información pública, así mismo puede contener información confidencial o legalmente protegida y está destinado únicamente para el uso del destinatario (s) previsto. Cualquier divulgación, difusión, distribución, copia o la toma de cualquier acción basada en la información aquí contenida está prohibido

**SOLICITUD DE INFORMACIÓN CON FOLIO NO.
070116524000021**

Identifique y señale en la tabla la siguiente información de su institución:

1. Número de Tratamientos (trámites o procedimientos) que realizan en los que utilizan datos personales
2. Número de personas que tienen acceso a los datos personales
3. Listado de Datos personales que utilizan.

Número de tratamientos que se llevan a cabo en los que utilizan datos personales.	Aproximadamente 73 tratamientos o procesos.
Número de personas que tienen acceso a los datos personales.	44 personas
Listado de datos personales que utilizan en la institución.	<ol style="list-style-type: none"> 1. Nombre de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros). 2. Firma. 3. CURP. 4. RFC. 5. Cédula Profesional. 6. Año de nacimiento o edad. 7. Beneficiarios. 8. Características físicas. 9. Circunstancias socioeconómicas. 10. Correo electrónico. 11. Currículum vitae. 12. Datos académicos. 13. Datos contenidos en declaraciones patrimoniales. 14. Datos de identificación. 15. Datos de salud. 16. Datos laborales. 17. Datos personales contenidos en documentos para acreditar personalidad del representante. 18. Datos personales contenidos en la identificación oficial presentada por la persona física. 19. Datos sobre procedimientos judiciales o seguidos en forma de juicio. 20. Descuentos personales (ahorro voluntario, hipoteca, seguro médico, seguro de automóvil entre otros). 21. Discapacidad.

Los datos personales recabados en este formato, serán protegidos, incorporados y tratados en los términos establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en los Lineamientos Generales para la Custodia y Protección de Datos Personales e Información Reservada y Confidencial en Posesión de los Sujetos Obligados del Estado de Chiapas y demás Normatividad aplicable.

La información de este documento así como la contenida en los documentos que se adjuntan, puede ser objeto de solicitudes de acceso a la información pública, así mismo puede contener información confidencial o legalmente protegida y está destinado únicamente para el uso del destinatario (s) previsto. Cualquier divulgación, difusión, distribución, copia o la toma de cualquier acción basada en la información aquí contenida está prohibido

**SOLICITUD DE INFORMACIÓN CON FOLIO NO.
070116524000021**

	<p>22. Domicilio.</p> <p>23. Huella digital.</p> <p>24. Lengua indígena.</p> <p>25. Menor de edad.</p> <p>26. Nacionalidad.</p> <p>27. Nivel educativo.</p> <p>28. Ocupación.</p> <p>29. Origen étnico o racial.</p> <p>30. Otros datos biométricos.</p> <p>31. Pertenencia a pueblo indígena.</p> <p>32. Sexo.</p> <p>33. Teléfono fijo o celular.</p> <p>34. Títulos profesionales.</p> <p>35. Población a impactar (LGBTIQ+).</p> <p>36. Nombre del Representante Legal.</p> <p>37. Primer Apellido del Representante Legal.</p> <p>38. Segundo Apellido del Representante Legal.</p> <p>39. Formato de autorización de uso de imagen.</p> <p>40. Formato de autorización de uso de imagen menor de edad.</p> <p>41. Datos financieros o bancarios.</p> <p>42. Estado de interdicción o incapacidad legal.</p> <p>43. Huella dactilar.</p>
--	--

"Los datos personales recabados en este formato, serán protegidos, incorporados y tratados en los términos establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en los Lineamientos Generales para la Custodia y Protección de Datos Personales e Información Reservada y Confidencial en Posesión de los Sujetos Obligados del Estado de Chiapas y demás Normatividad aplicable".

"La información de este documento así como la contenida en los documentos que se adjuntan, puede ser objeto de solicitudes de acceso a la información pública, así mismo puede contener información confidencial o legalmente protegida y está destinado únicamente para el uso del destinatario (s) previsto. Cualquier divulgación, difusión, distribución, copia o la toma de cualquier acción basada en la información aquí contenida está prohibido"