Documento de Seguridad para la Protección de Datos Personales

Boulevard Dr. Belisario Domínguez #1713 (Planta Baja) y 16 Poniente Sur, Colonia Xamaipak, C.P. 29067, Tuxtla Gutiérrez, Chiapas. Tel: 961 68 8672 cepsvypc@prevencion.chiapas.gob.mx centroprevencion@hotmail.com

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 LGPDPPSO, además de desarrollar buenas prácticas en la materia.

En ese sentido, el CEPSVyPC 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 CEPSVyPC, que integre las acciones interrelacionadas como lo dispone el artículo 34 de la LGPDPPSO, 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 CEPSVyPC 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.

Boulevard Dr. Belisario Domínguez #1713 (Planta Baja) y 16 Poniente Sur, Colonia Xamaipak, C.P. 29067, Tuxtla Gutiérrez, Chiapas.
Tel: 961 68 8672 cepsvypc@prevencion.chiapas.gob.mx
centroprevencion@hotmail.com

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 logar 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 CEPSVyPC, 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 duchas 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 CEPSVyPC
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
		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
		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
		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 CEPSVyPC 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.

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 CEPSVyPC 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 riegos de los datos personales que son objeto de tratamiento por el CEPSVyPC, 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, 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

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 CEPSVyPC 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 papelera 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.

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