SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES.

En la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, se establecen las bases, principios y procedimientos, para garantizar el derecho que tiene toda persona a la protección de sus datos personales en posesión de los sujetos obligados. La protección de datos personales implica una determinación, que se refiere a un derecho humano que es inherente a la persona; en la medida que éstos no pertenecen a la persona, sino que son la persona en sí misma. Ya que su identidad puede determinarse directa o indirectamente, a través de cualquier información, que posean los sujetos obligados.

Teniendo como base lo antes citado y de conformidad con el artículo 2, fracciones I, III, IV y VIII; artículo 3, fracciones I, II, III, IV, IX, XIII, XVII, XXV, XXVIII, XXIX y XXXI; artículo 20; además de los artículos del 27 al 36, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas. Se crea el presente documento en materia de protección de datos personales, con la finalidad de concientizar a las personas servidoras públicas, para recabar información precisa, de calidad y dar un adecuado trato a dichos datos. Ya que un mal tratamiento determina fuertes riesgos y hace peligrar la seguridad de los datos, que pueden ser utilizados de forma inadecuadas por terceros.

1.- Conceptos básicos en la materia.

En la aplicación del presente *Sistema de Gestión de Seguridad de Datos Personales*, se entenderá por:

Área u Órgano Administrativo: A la instancia de la Oficialía Mayor del Estado de Chiapas, que de acuerdo a sus funciones o atribuciones decide sobre el tratamiento de los datos personales;

Autoridad Garante: Transparencia para el Pueblo de Chiapas;

Aviso de Privacidad: Al documento puesto a disposición de la persona titular de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus Datos Personales, con el objeto de informarle los propósitos del tratamiento de los mismos;

Datos Personales: A cualquier información concerniente a una persona identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información;

Datos Personales Sensibles: A los datos que se refieran a la esfera más íntima de su titular o cuya utilización indebida pueda dar lugar a discriminación o conlleve un riesgo grave para esta. De manera enunciativa más no limitativa, se consideran sensibles los Datos Personales que puedan revelar aspectos como origen étnico o racial, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;

Documento de Seguridad: Al 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;

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

Medidas de Seguridad: Al conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los Datos Personales;

Oficialía: Oficialía Mayor del Estado de Chiapas;

Responsable: A la persona servidora pública titular del órgano administrativo designada por el titular de la Oficialía, quien decide de acuerdo a sus funciones o atribuciones sobre el tratamiento de datos personales;

SGSDP: Sistema de Gestión de Seguridad de Datos Personales

Titular: A la persona a quien corresponden o pertenecen los Datos Personales que son objeto de tratamiento;

Tratamiento: A cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los Datos Personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de Datos Personales;

2.- Objetivos y Alcances.

Objetivos:

- Determinar cómo están almacenados los datos.
- Determinar la organización de los archivos.
- Establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales.
- Garantizar la confidencialidad, integridad y disponibilidad de los datos.
- Eliminar o minimizar los riesgos, amenazas y posibles vulneraciones de los datos.

Alcances:

- La obtención de los datos personales a través de formatos físicos y digitales.
- El tratamiento de los datos personales a través de los Órganos Administrativos, con la finalidad de inscripción al Padrón de Proveedores del Poder Ejecutivo del Estado, participación en los procedimientos de adjudicación por licitaciones públicas, invitación restringida o adjudicación directa, celebrar contratos o pedidos de

adquisiciones, arrendamiento de bienes muebles y/o prestaciones de servicios, entrega de los bienes, pago de las obligaciones contractuales, comprobación del gasto público, cumplir con las obligaciones de transparencia, atender solicitudes de información en materia de transparencia, rendir informes, modificación de los contratos, rescisión de los contratos, suspensión o terminación anticipada del contrato, aplicación y cobro de las penas convencionales pactadas y aplicación y cobro de las garantías otorgadas.

- Los autorizados para el tratamiento de los datos personales, son las personas servidoras públicas adscritas a los Órganos Administrativos.
- La transferencia de los datos personales a las dependencias y/o entidades de la Administración Pública del Estado de Chiapas, a quienes se les contrata la adquisición de un bien o servicio.
- La unidad de almacenamiento portátil, archiveros o muebles con llave dentro de las oficinas de cada Órgano Administrativo será el lugar de almacenamiento de los datos personales

3.- Política de Gestión de los Datos Personales.

1. Tratar y recabar datos personales de manera lícita, conforme a las disposiciones establecidas por la Ley y demás normativa aplicable;
2. Sujetarse al tratamiento de datos personales al consentimiento del titular, salvo las excepciones previstas por la Ley;
3. Informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del Aviso de Privacidad;
4. Procurar que los datos personales tratados sean correctos y actualizados;
5. Suprimir los datos personales cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el Aviso de Privacidad y para las cuales se obtuvieron;
6. Tratar datos personales estrictamente el tiempo necesario para propósitos legales, regulatorios o legítimos para las cuales se obtuvieron;
7. Limitar el tratamiento de los datos personales al cumplimiento de las finalidades previstas en el Aviso de Privacidad;
8. No obtener los datos personales a través de medios fraudulentos;
9. Tratar lo menos datos personales posibles, y sólo aquéllos que resulten necesarios, adecuados y relevantes en relación con las finalidades previstas en el Aviso de Privacidad;
10. Establecer y mantener las medidas de seguridad;
11. Guardar la confidencialidad de los datos personales;
12. Identificar el flujo y ciclo de vida de los datos personales considerando: por qué medio se recaban, en qué procesos se utilizan, con quién se comparten y en qué momento y por qué medios se suprimen;
13. Mantener un inventario actualizado de los datos personales o de sus categorías que maneja el sujeto obligado;
14. Respetar los derechos de los titulares en relación con sus datos personales; y
15. Aplicar las excepciones contempladas en la normativa en materia de protección de datos personales;

4.- Las funciones y obligaciones del responsable, encargados y todas las personas que traten datos personales.

Para garantizar la aplicación correcta de este sistema, es necesario establecer los deberes de las personas servidoras públicas, que participan en el tratamiento de los datos personales derivado de sus atribuciones.

Al momento de recibir los datos personales la persona servidora pública, que se encargue de su recepción y tratamiento deberá:

1) Tener el Aviso de Privacidad.
2) Dar a conocer el Aviso de Privacidad al titular de los datos personales previo a la obtención de sus datos.
3) En caso de dudas o quejas de los titulares de los datos personales sobre el tratamiento de sus datos, orientar a la persona.
4) Al obtener los datos personales cerciorarse de que la información esté completa, actualizada, sea veraz y comprensible.
5) Comunicar discrepancias de los datos personales recabados al superior inmediato o a la persona que administra los datos personales.
6) Conocer y seguir las medidas de seguridad que le sean aplicables para el titular de los datos personales, durante el periodo en el que se posea los datos personales.
7) Obtener los datos personales para la finalidad para la cual estos fueron recabados según el trámite o el sistema de tratamiento que corresponda.
8) Tratar los datos personales de manera lícita siguiendo los principios establecidos en la Ley Estatal.
9) Conocer, aplicar y sujetarse al Aviso de Privacidad en el tratamiento de datos personales.
10) Guardar estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones.
11) Aplicar las medidas de seguridad correspondientes a los datos personales tratados y/o el sistema de protección en el que participa.
12) Abstenerse de realizar transferencias de datos personales que no vayan de conformidad con la finalidad para la cual se obtuvieron los datos.

La persona servidora pública responsable de cada sistema, o en su caso, la persona titular del Órgano Administrativo responsable de cada sistema, además de conocer la recepción y tratamiento de los datos deberá:

1) Aplicar medidas correctivas en caso de identificar incidentes, alteraciones o vulneraciones en el tratamiento de datos personales.
2) Informar al titular de los datos personales sobre los cambios que sufran los trámites y las transferencias nuevas que realicen de los datos personales.
3) Monitorear la implementación de las medidas de seguridad.
4) Levantar actas circunstanciadas de hechos ante la reincidencia de un incumplimiento en la aplicación de las medidas de seguridad.

5) Dar aviso al Comité de Transparencia, sobre las actas circunstanciadas de hechos levantadas por el incumplimiento del documento de seguridad y sobre el seguimiento de las mismas.
6) Presentar propuestas de mejora o modificación del documento de seguridad.
7) Emitir reportes en relación al tratamiento de los datos personales y la aplicación de medidas de seguridad.

5.- Inventario de Datos Personales.

Se debe establecer y mantener actualizado un inventario de los sistemas de tratamiento de datos personales, de conformidad a lo establecido en los Lineamientos Generales de Protección de Datos Personales para el Sector Público. Este inventario debe identificar o estar vinculado con la información básica, que permita conocer el tipo de tratamiento al que son sometidos los datos personales, la cual se relaciona de manera directa con su ciclo de vida, considerando los datos siguientes:

Datos de identificación.			
Fecha de elaboración.	Día	Mes	Año
Sujeto Obligado.	Oficialia Mayor del Estado de Chiapas		
Órgano Administrativo Responsable.			
Responsable del tratamiento de datos personales			
Finalidad de sistemas y los usos previstos.	• Inscripción al Padrón de Proveedores del Poder Ejecutivo del Estado. • Participación en los procedimientos de adjudicación por licitaciones públicas, invitación restringida o adjudicación directa. • Celebración del contrato o pedido. • Entrega de los bienes. • Pago de las obligaciones contractuales. • Comprobación del gasto público. • Cumplir con las obligaciones de transparencia. • Atender solicitudes de información en materia de transparencia. • Rendir informes. • Modificación de los contratos.		

	• Rescisión de los contratos. • Suspensión o terminación anticipada del contrato. • Aplicación y cobro de las penas convenciones pactadas. • Aplicación y cobro de las garantías otorgadas. • Los datos serán transferidos a las Dependencias y Entidades de la Administración Pública del Estado de Chiapas.
Nombre de la persona o personas sobre las cuales se obtienen los datos.	.
Datos personales sometidos a tratamiento.	• Credencial para votar. • Registro Federal de Contribuyentes. • Firma. • Número de teléfono celular. • Domicilio. • Correo electrónico.
Remisión o transferencia.	Dependencias y/o Entidades
Nombre del expediente	Formatos Físicos y Formatos Digitales.
Características del lugar de resguardo.	Unidad de almacenamiento portátil, archiveros o muebles con llave dentro de las oficinas de cada área.
Responsable del resguardo de los datos personales	
Fundamento legal	Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.

6.- Análisis de Riesgos.

Debido a las circunstancias generales, tanto físicas como humanas, en las que se tratan datos personales, hemos logrado identificar los siguientes riesgos posibles ante los que se pudiera enfrentar este Sujeto Obligado:

- Obtención de datos incompletos o incorrectos.
- Omitir la notificación al titular de los datos personales del Aviso de Privacidad.
- No difundir el Aviso de Privacidad.

- Ante la necesidad de tener un consentimiento expreso: no tener evidencia de que el titular de los datos personales conoce los términos del Aviso de Privacidad.
- No tener un lugar seguro y de acceso restringido en donde se puedan archivar los datos personales en físico.
- Permitir a toda persona servidora pública o personas ajenas a la dependencia, el acceso a los expedientes que contienen datos personales.
- Pérdida de expedientes físicos debido a catástrofes, inundaciones e incendios.
- Daño de la base de datos que contenga información confidencial.
- Fallas en los equipos de cómputo en donde se encuentran las bases de datos.
- Falta de capacitación de las personas servidoras públicas en relación a la confidencialidad que deben guardar sobre los datos personales que conozcan debido al desempeño de sus funciones.
- Pérdida, robo o extravío de expedientes.
- Alteración de la información.

Ante dichos riesgos identificados es necesario hacer un análisis de dichos riesgos, amenazas y sus posibles vulneraciones.

Amenaza	Vulnerabilidades	Posibles consecuencias
Acceso de personas no autorizadas a los sistemas.	Adquirir información datos personales.	Divulgación de datos personales, robo de información o modificaciones no autorizadas.
Acceso de personas como criminales o traficantes de datos a los sistemas o plataformas oficiales.	Adquirir datos personales para utilizarlos con fines de explotación, chantaje, extorsión o cualquier uso criminal.	Extorsiones, ataques a personas, robo de información, vulneración a la seguridad física y mental de los ciudadanos.
Personal del sujeto obligado con poco conocimiento sobre el tratamiento de datos personales.	Obtener información para beneficio personal, curiosidad, error involuntario o por fines económicos.	Ataque a otras personas servidoras públicas, robo de información, pérdida de datos personales, uso indebido de datos personales, extorsión o modificaciones no autorizadas.
Daño físico.	Agua, fuego, accidentes o corrosión.	Daño o pérdida de los datos personales.

Eventos naturales.	Desastres climatológicos, fenómenos meteorológicos, sismos o cualquier eventualidad por causa natural.	Daño o pérdida de los datos personales.
Fallas técnicas.	Pérdida de electricidad, falla o pérdida de internet, falla en sistemas, correos electrónicos o plataformas oficiales.	Daño o pérdida de los datos personales, divulgación, transferencia de datos personales o modificaciones no autorizadas.
Decadencias técnicas.	Mantenimiento insuficiente, falla en equipos, cambios de voltaje, poca o absoluta renovación de equipos de telecomunicaciones o cómputos.	Pérdida, destrucción y daño.
Susceptibilidad en redes o sistemas autorizados.	Falta de contraseñas altamente efectivas, actualización de antivirus, falta de mecanismos para identificar o autenticación de usuarios.	Pérdida, destrucción, daño, divulgación y transferencia de datos personales, modificaciones no autorizadas o robo de información.
Organización.	Procesos carentes de formalidad para administración, acceso, uso y proceso de archivo.	Pérdida, destrucción, daño, divulgación y transferencia de datos personales, modificaciones no autorizadas o robo de información.
Espacio donde se archiven.	Carencia de espacio, espacio con poca seguridad, espacio no adecuado, falta de llaves o medidas de seguridad para accesos.	Daño o pérdida de los datos personales, divulgación y transferencia de datos personales, modificaciones no autorizadas o robo de información.
Daño y/o alteración de la base de datos que contenga información confidencial.	Carencia de un servidor o sistema que almacene los datos personales, la falta de registros, controles o bitácoras, para regular la entrada y salida de personal autorizado, al área donde se almacenan o archivan los datos personales (en su caso los expedientes que los contengan), es un escenario de vulneración y riesgo, facilitando el mal manejo de los datos	Daño de los datos personales, pérdida de los datos personales o modificaciones no autorizadas.

	personales y la pérdida, robo o extravío de expedientes.	

7.- Identificación de las Medidas de Seguridad y Análisis de Brecha.

Una vez identificados los posibles riesgos, así como las amenazas, vulnerabilidades y escenarios de incidentes de los datos personales, a los que este Sujeto Obligado se encuentra susceptible de enfrentar, podemos realizar el análisis de brecha de las medidas de seguridad:

Medidas de seguridad existentes:

- Quien recaba los datos personales, es una persona servidora pública del área, asignada especialmente para recabar datos en general, necesarios para cada trámite.
- El espacio físico o área donde se recaban datos personales, es dentro de las instalaciones de la Oficialía Mayor.
- Cuando los datos personales son recabados de forma digital, se realiza por medio de plataformas oficiales o correo electrónico oficial.
- En la mayoría de las áreas, el acceso se tiene restringido, una vez que el dato se encuentra en posesión de la persona servidora pública, estos se colocan fuera del alcance de toda persona no autorizada.
- Cada oficina cuenta con puertas que separan el área al momento de terminar labores.
- Las llaves que se tienen de cada área se encuentran en manos de las personas servidoras públicas acreditadas por cada área.
- Una vez recabados los datos personales, la persona servidora pública genera un expediente para cada trámite o servicio, ya sea en físico o electrónico.
- Una vez recabados los datos personales e integrados a la carpeta o expediente en físico o electrónico y guardada está en archiveros o puesta en resguardo, solo tendrán acceso las personas servidoras públicas del área.
- Una vez recabados los datos personales, en caso de que se les dé proceso electrónico, la persona servidora pública guardara los mismos en carpeta electrónica, ya sea en su computadora, carpeta compartida, correo electrónico oficial o plataforma.
- Una vez concluido el trámite, los datos personales recabados se dejan intactos en la carpeta, archivo o expediente del trámite al que pertenecen.
- Cada carpeta de trámites o archivo, al terminar el proceso de cada uno, son resguardados en cada área.

Las medidas de seguridad que actualmente se llevan a cabo pudieran ser efectivas de aplicarse de manera continua y consciente en las áreas administrativas del sujeto obligado. El riesgo latente que se provoca por la falta de conocimiento o compromiso para la aplicación de estas medidas existentes, se puede minimizar por medio del establecimiento obligatorio de dichas medidas de seguridad y de la mejora continua de las mismas.

8.- Medidas de Seguridad.

Se deben seleccionar los controles de seguridad faltantes identificados en el análisis de brecha y en el análisis de riesgos, con el objetivo de seleccionar los controles apropiados y justificados para satisfacer la valoración del riesgo. Los controles pueden proporcionar uno o más de los siguientes tipos de protección:

- ☐ Corrección.
- ☐ Eliminación.
- ☐ Prevención.
- ☐ Minimización del impacto.
- ☐ Monitoreo.
- ☐ Concienciación.

Por ejemplo:

- Las personas servidoras públicas que tienen contacto con el titular de los datos personales por sus funciones, deben realizar un listado de las personas servidoras públicas que recaban datos personales.
- Las personas servidoras públicas que recaban datos personales deberán forzosamente asistir a por lo menos a una capacitación en materia de datos personales impartida por el Área de Transparencia.
- Para evitar el riesgo de obtener datos personales incompletos o incorrectos, la persona servidora pública autorizada para recabarlos, deberá pedir a la persona titular de los datos, que acredite su personalidad.
- Los datos personales recabados deberán ser recibidos únicamente en las instalaciones de cada área.
- Al concluir la jornada laboral, se deberá guardar los expedientes, para no dejarlos al alcance de personas no autorizadas.
- El área específica donde se recaben los datos deberá contar con puertas que tengan llave, sin excepción alguna, para asegurar de forma efectiva el trato adecuado de los datos personales, así evitar mal uso de los mismos o vulneraciones.
- Al término de las labores, deberá cerrarse cada oficina de las áreas, para evitar el contacto de personas no autorizadas, con los datos personales recabados.
- Para evitar riesgos, respecto a los expedientes electrónicos, se debe contar con un respaldo electrónico. Dicho respaldo deberá realizarse, como mínimo, de manera anual.
- Se deberá crear por cada área, un control o bitácora con las personas servidoras públicas que tienen acceso al archivo, mismo que debe contener lo siguiente:

    a) Registro para anotar el nombre y puesto de la persona servidora pública autorizada.
    b) Fecha, hora de entrada y hora de salida del archivo.
    c) Registrar el expediente que se consultó.
    d) Registrar el expediente que se extrae del archivo, y fecha en la que se regresa el expediente.

e) Firma de conformidad de la persona servidora pública que consultó el expediente.
f) Firma de consentimiento de la persona servidora pública autorizada para llevar el control de este archivo.

- Cada área del sujeto obligado deberá elaborar controles de archivo, conforme a sus procesos institucionales. Esto es, un inventario de documentos que se mandan al Área Coordinadora de Archivo para su resguardo.
- En caso de ser necesario derivado de las funciones de las personas servidoras públicas, o por requisito del trámite, se deba realizar una transferencia de datos personales, se deberá informar al sujeto que reciba los datos el Aviso de Privacidad para que se sujete al mismo.
- El área que reciba los datos personales deberá encargarse de la supresión de los datos que reciba cuando esta corresponda.
- El tercero que reciba los datos personales deberá sujetarse a las finalidades y lineamientos del Aviso de Privacidad de este sujeto obligado y deberá adoptar las medidas de seguridad previstas en este documento. En caso de ser necesario conforme a las disposiciones normativas, se deberá firmar un convenio o acuerdo de confidencialidad que proteja el tratamiento de los datos personales que recaba este sujeto obligado y transfiere al tercero.
- En los casos en los cuales se realicen clasificaciones de información confidencial, que incluyan datos personales, los documentos que contengan los datos, deberán entregarse siempre en versión pública, adjuntando índice de datos personales.
- Al momento de finalizar el trámite, todos los expedientes, deberán enviarse al archivo, conforme a la normatividad correspondiente.

Medidas de protección en caso de vulneraciones a la seguridad:
En caso de ocurrir alguna vulneración deberá registrarse en la bitácora de contingencias, por ejemplo:

Fecha en la que ocurrió	Motivo	Las acciones correctivas implementadas de forma inmediata y definitiva
30/04/2026	Huracán.	Impresión del expediente y generar nuevo expediente electrónico.

Después del registro, se deberá informar de forma inmediata al titular y a la Autoridad Garante, de las vulneraciones de seguridad ocurridas, las que afecten o impacten de forma significativa los derechos patrimoniales o morales del titular, en cuanto se confirmen y este en proceso las acciones encaminadas para dimensionar la afectación, con la finalidad de que las personas titulares afectadas puedan tomar las medidas correspondientes para la defensa de sus derechos, dicha notificación debe contener lo siguiente:

I. La naturaleza del incidente.

II. Los datos personales comprometidos.
III. Las recomendaciones y medidas que el titular puede adoptar para proteger sus intereses.
IV. Las acciones correctivas realizadas de forma inmediata.
V. Los medios donde puede obtener mayor información al respecto.

Al ocurrir una vulneración de seguridad, la persona servidora pública titular del área responsable y/o el responsable del sistema deberá analizar la causa por lo que ocurrió dicha vulneración, e implementar y anexar a su plan de trabajo las acciones preventivas y correctivas para adecuar medidas de seguridad que prevengan esta eventualidad, para evitar que la vulneración se repita. El responsable deberá establecer controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales, guarden confidencialidad respecto de éstos, obligación que subsistirá aún después de finalizar sus relaciones con el mismo.

9.- Revisiones y Auditoría

Revisión de los Factores de Riesgo.

Se debe monitorear y revisar el riesgo con sus factores relacionados, es decir, el valor de los activos, las amenazas, vulnerabilidades, el impacto, y la probabilidad de ocurrencia, para identificar en una etapa temprana cualquier cambio en el contexto del alcance y objetivos y así mantener una visión general de la imagen del riesgo.

El riesgo no es estadístico: Las amenazas, vulnerabilidades, probabilidad y consecuencias pueden cambiar abruptamente sin previo aviso. Esta situación exige la revisión de cada riesgo por separado, así como la suma de ellos, para conocer el impacto potencial acumulado de las amenazas. Por lo tanto, se requiere de constante monitoreo para detectar esos cambios.

Los siguientes puntos deberán estar continuamente monitoreados:

- Verificar de primera mano la aplicación, actualización e impacto de las medidas de seguridad aplicadas.
- Monitorear avances, aplicación, eventualidades y novedades respecto a la aplicación de las medidas de seguridad.
- Incidentes y vulneraciones de seguridad.
- Modificaciones necesarias a los activos, por ejemplo, cambio o migración tecnológica.
- Nuevas amenazas que podrían estar activas dentro y fuera del sujeto obligado y que no han sido valoradas.
- Amenazas nuevas o pasadas que vuelven a surgir.

Auditoría.

La auditoria interna monitorea y revisa la eficacia y eficiencia del Sistema de Gestión de Seguridad de Datos Personales (SGSDP), indica explícitamente cualquier tratamiento de datos personales interno y externo del sujeto Obligado, responsables, recursos, criterios a utilizar durante la auditoria, así como los procesos y/o áreas que serán auditadas.

Como resultado de una auditoría se deben obtener observaciones sobre riesgos existentes para aplicar medidas preventivas, es decir, controles para que no ocurra una vulneración, así como observaciones sobre puntos que requieren medidas correctivas inmediatas.

10.- Mejora continua y capacitación

En esta fase, se adoptan las medidas correctivas y preventivas en función de los resultados de la revisión o verificación efectuadas, o de otras informaciones relevantes, para lograr la mejora continua.

Mejora Continua

El monitoreo de los factores de riesgo, así como los resultados de las auditorías proporcionan información para demostrar la eficacia del SGSDP, pero también presentan las áreas de oportunidad donde éste puede ser mejorado. Los puntos de mejora del SGSDP pueden corresponder a dos tipos:

a) Acciones correctivas. Son las acciones encaminadas a eliminar las causas de fallas o incidentes ocurridos en el SGSDP, con objeto de prevenir que vuelvan a ocurrir, dichas acciones deben ser proporcional a la gravedad del incidente.

Las acciones correctivas deben atenderse considerando:

I. El análisis y revisión de la falla o incidente;
II. Determinar las causas que dieron origen a la falla o incidente;
III. Evaluar las acciones necesarias para evitar que la falla o incidente vuelva a ocurrir;
IV. Determinar e implementar las acciones necesarias;
V. Registrar los resultados de las acciones tomadas; y
VI. Revisar la eficacia de las acciones correctivas tomadas.

b) Acciones preventivas. Son las acciones encaminadas a eliminar las causas de fallas o incidentes posibles en el SGSDP, dichas acciones deben ser proporcionales a las amenazas potenciales.

Las acciones preventivas deben atenderse considerando:

I. El análisis y revisión de la amenaza;
II. Determinar las fallas o incidentes que podría desencadenarse con una amenaza;
III. Evaluar las acciones necesarias para evitar que la falla o incidente ocurra;

IV. Determinar e implementar las acciones necesarias;
V. Registrar los resultados de las acciones tomadas; y
VI. Revisar la eficacia de las acciones preventivas tomadas.

La implementación de las acciones preventivas o correctivas puede establecerse en un periodo inmediato a la detección y análisis del punto de mejora o calendarizarse para una futura revisión del SGSDP en función de la importancia de la mejora y los recursos disponibles.

La eficacia de las acciones preventivas y correctivas se evalúa considerando la reducción de los niveles de riesgo en los resultados del monitoreo a los SGSDP o de auditorías posteriores.

Capacitación.

La mejor medida de seguridad contra posibles vulneraciones es contar con personal consciente de sus responsabilidades y deberes respecto a la protección de datos personales y que identifiquen cuál es su contribución para el logro de los objetivos del SGSDP. Por ello, se deben establecer y mantener programas de capacitación como:

a) *Concienciación:* Difusión en general de la protección de datos personales en la organización;
b) *Entrenamiento:* Capacitar al personal de manera específica respecto a sus funciones y responsabilidad en el tratamiento y seguridad de los datos personales; y
c) *Educación:* Incluir la seguridad en el tratamiento de los datos personales dentro de la cultura de los servidores públicos.

Se debe realizar una detección de necesidades para identificar el nivel y tipo de capacitación necesaria para el personal, de acuerdo con las responsabilidades asignadas y tomando en cuenta su perfil de puesto, especialmente de aquéllos involucrados en el tratamiento de datos personales.

Síntesis de la Implementación del SGSDP

En esta sección se presenta una síntesis de los pasos del proceso de implementación de un SGSDP, para que los responsables la usen como una referencia rápida del contenido total de este documento.

Paso 1. Conceptos básicos en la materia: Conceptos esenciales que facilitan el aprendizaje, la organización y el análisis de la información para la implementación del SGSDP.

Paso 2. Alcance y Objetivos: Consideraciones respecto al tratamiento de datos personales y el modelo de negocios de la organización.

Paso 3. Política de Gestión de Datos Personales: El compromiso formal documentado de las personas servidoras públicas para el tratamiento adecuado de datos personales.

Paso 4. Funciones y Obligaciones de Quienes Traten Datos Personales: Asignación de responsabilidades para la implementación del SGSDP.

Paso 5. Inventario de Datos Personales: Identificación de la cantidad, tipos de datos y donde se encuentran resguardados.

Paso 6. Análisis de Riesgo de los Datos Personales: Proceso para identificar los escenarios de riesgo prioritarios y darles tratamiento proporcional, se compone de los siguientes pasos:

- Identificar Amenazas.
- Identificar Vulnerabilidades.
- Identificar Escenarios de Consecuencias.

Paso 7. Identificación de las Medidas de Seguridad y Análisis de Brecha: Proceso de evaluación de las medidas de seguridad que ya existen en la organización contra las que sería conveniente tener. Los controles de seguridad, deben considerar lo siguiente:

- Políticas del SGSDP.
- Cumplimiento legal.
- Clasificación y acceso de los activos.
- Seguridad del personal.
- Desarrollo y mantenimiento de sistemas.
- Vulneraciones de seguridad.

Paso 8. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales: Se deben seleccionar los controles de seguridad faltantes identificados en el análisis de brecha y en el análisis de riesgos, con el objetivo de seleccionar los controles apropiados y justificados para satisfacer la valoración del riesgo.

Paso 9. Revisiones y Auditoría: Proceso de revisión del funcionamiento del SGSDP respecto a la política establecida, cada vez que exista un cambio en el contexto del alcance y objetivos del SGSDP, deberá considerar lo siguiente:

- Revisión de los Factores de Riesgo. Consideraciones para monitorear el estado del riesgo y aplicar las modificaciones pertinentes para mejorar el SGSDP.
- Auditoría. Requerimientos para los procesos de auditoría interna/externa.

Paso 10. Mejora Continua y Capacitación: Consideraciones para incluir la protección de datos en la cultura de los servidores públicos y mantener siempre actualizado el SGSDP:

- Mejora Continua. La aplicación de medidas preventivas y correctivas sobre el SGSDP.
- Capacitación. Programas de mejora en el personal para mantener la vigencia del SGSDP.

Paulina Eunice Méndez Meza
Titular de la Unidad de Asuntos Jurídicos y Presidenta del Comité de Transparencia.

Jose Domingo Ocaña Clemente
Titular del Área de Transparencia y Secretario Técnico del Comité de Transparencia

Marisa Oliva Cordero Zúñiga
Titular de la Dirección de Adquisiciones de Bienes y Servicios, Responsable del Área Coordinadora de Archivo y Vocal del Comité de Transparencia.

HOJA PROTOCOLARIA DE FIRMAS DEL **ANEXO** CORRESPONDIENTE AL ACTA DE LA DÉCIMA TERCERA SESIÓN DEL COMITÉ DE TRANSPARENCIA, QUE CELEBRAN LA PRESIDENTA, EL SECRETARIO TÉCNICO Y LA VOCAL DEL COMITÉ DE TRANSPARENCIA, DE FECHA 16 DE JUNIO DE 2026.