DOCUMENTO DE SEGURIDAD

EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LA SECRETARÍA DE HACIENDA

CONTENIDO

DOCUMENTO DE SEGURIDAD

o INTRODUCCIÓN

En observancia al cumplimiento a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de Chiapas, la Secretaría de Hacienda (Secretaría), ha diseñado el presente documento de seguridad, el cual tiene como finalidad la de controlar internamente el total de sistemas de datos personales que posee la Secretaría, los tipos de datos personales que contiene cada uno, los encargados, usuarios de cada sistema y las medidas de seguridad físicas, administrativas y tecnológicas que se hayan implementado, además de establecer parámetros mediante un conjunto de procesos y sistemas diseñados, administrados por la Secretaría en todas las áreas que integran la Secretaría y que traten datos. De esta manera, la gestión de la seguridad de la información que contenga datos personales, formará parte de un sistema administrativo que busca establecer, implementar, operar, monitorear y mejorar los procesos y sistemas relativos a la confidencialidad, integridad y disponibilidad de la información, aplicando un enfoque basado en los riesgos que esta Secretaría afronta.

Para su desarrollo del presente documento, la Secretaría como responsable, identificó cada uno de los procesos que conlleva el tratamiento de los datos personales que se llevan a cabo dentro de esta, para así establecer las medidas y/o acciones a implementar en cada una de las áreas, a partir de las finalidades del tratamiento, con base en las funciones que se desempeñan en estas.

Por último, es imperante mantener actualizado el documento de seguridad lo que traerá como resultado reducir brechas de vulnerabilidad al implementar las medidas de seguridad adoptadas al tratamiento de los datos personales, el análisis de riesgo y brecha, que permiten y minimizar los riesgos a través de capacitación continua que permita comprender la importancia de adoptar medidas para la prevención de las vulneraciones a los datos personales.

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.

Por otra parte es necesario mencionar que la Constitución Política de los Estados Unidos Mexicanos en los artículos 6 y 16 incorpora el derecho de toda persona a la protección de sus datos personales, así como al acceso, rectificación, cancelación y oposición en los términos que determina la ley.

El presente Documento de Seguridad tiene como propósito establecer el marco de referencia del tratamiento de los datos personales que se llevan a cabo al interior de la Secretaría de Hacienda del Estado por las diversas órganos administrativos que conforman su estructura orgánica, para mantener vigente y promover la mejora continua en la protección de los mismos, en términos de lo previsto en los

artículos 35 y 36 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), así como los artículos 49 y 50 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas además de desarrollar buenas prácticas en la materia.

Considerando que los datos personales constituyen el principal activo de información objeto del presente documento, es necesario señalar que todos y cada uno de los elementos que lo integran, constituyen un sistema interno para la gestión y tratamiento de los datos personales en posesión de la Secretaría de Hacienda, por lo que en este trabajo se incluye también al Sistema de Gestión de esta Secretaría con la finalidad de poner a disposición la 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. Dicho lo anterior, el presente documento se integra a partir 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.

Por lo anterior, esta Secretaría, con la finalidad de establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, emite el presente documento, en observancia de los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los datos personales, con la intención de brindar homogeneidad en la dependencia en los procesos para la protección de los datos personales de la Secretaría. Asimismo, el presente documento tiene como propósito controlar internamente el universo de datos personales en posesión de esta responsable, el tipo de datos personales que contienen los sistemas, las obligaciones, el análisis de riesgos y los mecanismos de monitoreo y revisión de las medidas de seguridad, entre otros.

Para dar cumplimiento a lo anterior y de conformidad con lo dispuesto en la LGPDPPSO, el documento deberá contener, al menos, la siguiente información:

I. El inventario de datos personales y de los sistemas de tratamiento;
II. Las funciones y obligaciones de las personas que traten datos personales;
III. El análisis de riesgos;
IV. El análisis de brecha;
V. El plan de trabajo;
VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y
VII. El programa general de capacitación.

Alcances del documento de seguridad y del Sistema de Gestión

Este documento se aplica a todas las áreas de la Secretaría de Hacienda que realicen o efectúen tratamientos de datos personales en ejercicio de sus atribuciones, facultades o funciones, los cuales estarán bajo su estricta responsabilidad, tanto en los espacios físicos como en los medios electrónicos en los que los resguarden, operen y administren, en observancia a los principios, deberes y obligaciones que prevén la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) , Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas (LPDPPSOCHIS) y los Lineamientos para la Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas (Lineamientos) .

De acuerdo a lo que dispone el Reglamento Interior de la Secretaría en su artículo 7, esta Dependencia se estructura con los siguientes Órganos Administrativos:

I.- Unidades de Apoyo

a) Unidad de Apoyo Administrativo.

b) Unidad de Informática.

c) Unidad de Planeación.

d) Unidad de Coordinación Administrativa de Organismos Públicos.

e) Unidad Técnica.

f) Unidad de Inteligencia Patrimonial y Económica.

g) Unidad de Transparencia.

h) Unidad de Vinculación de Atención a Auditorías.

i) Unidad de Archivo.

II. Subsecretaría de Planeación.

III. Subsecretaría de Egresos.

IV. Subsecretaría de Ingresos.

V. Tesorería Única.

VI. Coordinación General de Recursos Humanos.

VII. Procuraduría Fiscal.

Glosario de Términos

Las siguientes definiciones se retoman de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, el Diccionario de Protección de Datos Personales, y la Guía para Implementar un Sistema de Gestión de Seguridad de Datos Personales Junio 2015.

Aceptar el riesgo: Decisión informada para coexistir con un nivel de riesgo.

Activo: En términos generales, un activo es cualquier elemento que representa un valor para la organización. Según la Real Academia Española, «valor» se define como: a) grado de utilidad o aptitud de las cosas para satisfacer las necesidades o proporcionar bienestar o deleite, y b) cualidad de las cosas, en virtud de la cual se da por poseerlas cierta suma de dinero o equivalente.

Análisis de riesgos: Permite identificar los peligros y evaluar el nivel de riesgo hacia los datos personales. Las metodologías de análisis de riesgo establecen un proceso sistemático que consiste en crear escenarios de riesgo, identificando y correlacionando todos los elementos que intervienen en él: activo (que en el presente contexto consiste en los datos personales), amenazas, vulnerabilidades, controles existentes e impactos o consecuencias. Una vez creados los escenarios de riesgo, se procede a evaluar cualitativa o cuantitativamente el riesgo mediante el establecimiento de parámetros como la probabilidad de ocurrencia y el nivel de impacto o de beneficio para el atacante.

Amenaza: Circunstancia o evento con la capacidad de causar daño a una organización.

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 y encargadas de los datos personales.

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

Bloqueo: Identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, 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 período, los datos

personales no podrán ser objeto de tratamiento. Transcurrido éste, se procederá a su cancelación en la base de datos que corresponda.

Confidencialidad: Propiedad de la información para no estar a disposición o ser revelada a personas, entidades o procesos no autorizados.

Comité de Transparencia: Instancia a la que hace referencia el artículo 43 de la Ley General de Transparencia y Acceso a la Información Pública.

Compartir el riesgo: Proceso donde se involucra a terceros para mitigar la pérdida generada por un riesgo en particular, sin que el dueño del activo afectado reduzca su responsabilidad.

Comunicar el riesgo: Compartir o intercambiar información acerca del riesgo; esto entre la alta dirección, custodios y demás involucrados.

Custodios: Aquellas personas servidoras públicas con responsabilidad funcional sobre los activos: responsables del departamento de datos, administradores de sistemas o responsables de un proceso o proyecto específico, entre otros.

Datos personales: Cualquier información concerniente a una persona física 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: Los que se refieran a la esfera más íntima de la persona titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De modo enunciativo más no limitativo, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

Documento de seguridad: Instrumento que describe y da cuenta de modo 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.

Disponibilidad: Propiedad de un activo para ser accesible y utilizable cuando lo requieran personas, entidades o procesos autorizados.

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

Evitar el riesgo: Acción para retirarse de una situación de riesgo o decisión para no involucrarse en ella.

Identificar el riesgo: Proceso para encontrar, enlistar y describir los elementos del riesgo. Impacto: Una medida del grado de daño a los activos o cambio adverso en el nivel de objetivos alcanzados por una organización.

Incidente: Escenario donde una amenaza explota una vulnerabilidad o conjunto de vulnerabilidades.

Integridad: La propiedad de salvaguardar la exactitud y completitud de los activos.

Reducir el riesgo: Acciones tomadas para disminuir la probabilidad, las consecuencias negativas, o ambas, asociadas al riesgo.

Responsable: Los sujetos obligados (a los que se refiere el artículo 1° de la Ley General) que deciden sobre el tratamiento de datos personales.

Retención del riesgo: Aceptación de la pérdida generada por un riesgo en particular. Esta acción implica monitoreo constante del riesgo retenido.

Riesgo: Combinación de la probabilidad de un evento y su consecuencia desfavorable.

Riesgo de seguridad: Combinación de la posibilidad de que se materialice una amenaza y sus consecuencias negativas.

Riesgo inherente: Riesgo intrínseco al activo, sin considerar las medidas de seguridad implementadas.

Riesgo residual: El riesgo remanente después de tratar el riesgo.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información, así como otras propiedades delimitadas por la normatividad aplicable.

Sistema de Gestión de Seguridad de Datos Personales (SGSDP): Sistema de gestión general para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales en función del riesgo de los activos y de los principios básicos de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad previstos en la Ley General, los Lineamientos Generales, normatividad secundaria y cualquier otro principio que la buena práctica internacional estipule en la materia.

Sujeto obligado: Son sujetos obligados por la Ley General. En el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.

Titular: Persona física a quien corresponden los datos personales. Tratamiento: 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.

Transferencia: Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, responsable o encargado. Tratar el riesgo: Procesos que se realizan para modificar el nivel de riesgo.

Unidad de Transparencia: Instancia a la que hace referencia el artículo 45 de la Ley General de Transparencia y Acceso a la Información Pública.

Valorar el riesgo: Proceso para asignar valores a la probabilidad y consecuencias del riesgo.

Vulnerabilidad: Falta o debilidad de seguridad en un activo o grupo de activos que puede ser explotada por una o más amenazas.

- **OBJETIVO**

El presente documento tiene por objeto describir el tratamiento de la seguridad física y la aplicación de las disposiciones legales comprendidas en la materia de protección de datos personales, que recaba la Secretaría de Hacienda. Así mismo este documento ofrece el marco de trabajo para la protección de los datos personales en posesión de esta, ya que, de acuerdo a las disposiciones legales de la materia, este documento de seguridad es el 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; los cuales establecen los elementos y actividades de gestión para la operación y control de los procesos que impliquen el tratamiento de datos personales, con el objeto de protegerlos de manera sistemática y continua, y promover la adopción de mejores prácticas en relación con la protección de datos personales.

Marco normativo

- Artículos 6, apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos (CPEUM).

- Artículo 3 de la Constitución Política del Estado Libre y Soberano de Chiapas.

- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) .

- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas (LPDPPSOCHIS).

- Lineamientos para la Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas (Lineamientos) .

o ALCANCE DEL DOCUMENTO DE SEGURIDAD

De acuerdo a lo que dispone el Reglamento Interior de la Secretaría en su artículo 7, esta Dependencia se estructura con los siguientes Órganos Administrativos:

a) Unidad de Apoyo Administrativo.

b) Unidad de Informática.

c) Unidad de Planeación.

d) Unidad de Coordinación Administrativa de Organismos Públicos.

e) Unidad Técnica.

f) Unidad de Inteligencia Patrimonial y Económica.

g) Unidad de Transparencia.

h) Unidad de Vinculación de Atención a Auditorías.

i) Unidad de Archivo.

II. Subsecretaría de Planeación.

III. Subsecretaría de Egresos.

IV. Subsecretaría de Ingresos.

V. Tesorería Única.

VI. Coordinación General de Recursos Humanos.

VII. Procuraduría Fiscal.

Los órganos administrativos que se acaban de enlistar deberán observar en todas y cada una de sus partes, el cumplimiento del Programa de Protección de Datos Personales.

Asimismo el documento de seguridad se aplicará a los órganos administrativos de esta Secretaría que realicen tratamientos de datos personales en ejercicio de sus atribuciones, y a todos los tratamientos de datos personales que efectúen con observancia de los principios, deberes y obligaciones que establece la ley de la materia.

Sistema de gestión de los datos personales en posesión de la Secretaría de Hacienda

Para el tratamiento de los datos personales que lleva a cabo la Secretaría de Hacienda a través de su obtención, uso, registro, conservación, acceso, manejo, aprovechamiento, transferencia, disposición o cualquier otra operación aplicable a los mismo, se realiza el establecimiento de políticas y métodos orientados a salvaguardar su confidencialidad, integridad y disponibilidad, conforme a los preceptos previstos por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y la Ley General de Transparencia y Acceso a la Información Pública. En tal virtud, la Secretaría de Hacienda inició su proceso de planificación de los esquemas de protección de datos mediante la identificación de todos y cada uno de los procesos y tareas en los que, de acuerdo con el ámbito de funciones de las distintas áreas que conforman a esta Dependencia, se involucra el tratamiento de datos personales. Para ello, se dispuso de un formato que permitió a las diversas unidades administrativas realizar el levantamiento de inventarios de los datos personales que se encuentran bajo su responsabilidad, considerando los elementos:

SECRETARÍA DE HACIENDA
GOBIERNO DE CHIAPAS
2022: Año de Ricardo Flores Magón, Precursor de la Revolución Mexicana"

Documento de Seguridad de la Secretaría de Hacienda

(Artículo 50 fracciones I, II, V y VII)

Órgano Administrativo:

Nombre del Sistema	
Objetivo del Sistema	
Fundamento Legal	
Datos personales solicitados	
Nombre del administrador del sistema	
Cargo del administrador del sistema	
Ubicación del sistema y características físicas del lugar	
Usuario	Ciudadano ☐ Servidor Público ☐
Total de Datos:	
Medidas de seguridad actuales implementadas al sistema:	

Es así que a través del desarrollo de un instrumento estandarizado, se llevó a cabo el levantamiento del inventario de datos, con el propósito de identificar, entre otros aspectos, la categoría y tipo 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 al tratamiento, 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 ese 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 los datos, éstos deben ser sometidos a un proceso de bloqueo y, en su caso, de cancelación, supresión o destrucción. De igual forma, una vez integrados los inventarios de datos, se dispuso de la 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, los factores de riesgo a los que eventualmente se encuentran expuestos. Con base en dicho análisis de riesgo, 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 y, 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 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. Como parte del sistema de gestión y política de seguridad institucional, se enmarcan las reglas generales siguientes:

a) Tratar datos personales de manera lícita, conforme a las disposiciones establecidas por la Ley General y local de la materia;

b) Sujetar el tratamiento de los datos personales al principio de consentimiento, salvo las excepciones previstas por la Ley;

c) Informar a los titulares del tratamiento de los datos y sus finalidades;

d) Procurar que los datos personales tratados sean correctos y estén actualizados;

e) Suprimir los datos personales cuando hayan dejado de ser necesarios para las finalidades para las cuales se obtuvieron;

f) Tratar los datos personales estrictamente para propósitos legales o legítimos de la Secretaría de Hacienda;

g) Limitar el tratamiento de los datos personales al cumplimiento de las finalidades;

h) Respetar la expectativa razonable de privacidad del titular;

i) Tratar estrictamente los datos personales necesarios, adecuados y relevantes en relación con las finalidades;

j) Velar por el cumplimiento de los principios;

k) Establecer y mantener medidas de seguridad;

l) Guardar la confidencialidad de los datos personales;

m) Identificar el flujo y ciclo de vida de los datos personales;

n) Mantener actualizado el inventario de datos personales o de las categorías que maneja la Secretaría de Hacienda;

o) Respetar los derechos de los titulares en relación con sus datos personales;

p) Aplicar las excepciones contempladas en la normativa en materia de protección de datos personales, y;

q) Identificar a los servidores públicos de la Secretaría de Hacienda responsables del tratamiento de los datos personales.

Con base en lo anterior, la Secretaría de Hacienda determina las pautas de acción del personal encargado de tratamiento de datos personales con miras a generar su correcto resguardo, buscando en todo momento actuar en apego a las directrices de la LGPDPPSO, siempre en consideración de la salvaguarda del derecho a la privacidad y protección de datos de las personas.

En cumplimiento a lo establecido en el artículo 50 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, el cual establece los elementos por los que se integra el documento de seguridad, se tiene lo siguiente:

Fracciones I, II, III, IV, V, XII:

I. **El nombre de los sistemas de tratamiento o base de datos personales**

II. **El nombre, cargo y adscripción del administrador de cada sistema de tratamiento y/o base de datos personales.**

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

IV. **El inventario de los datos personales tratados en cada sistema de tratamiento y/o base de datos personales.**

En cumplimiento a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, en específico el artículo 50 en las fracciones I y V, la Secretaría de Hacienda identificar que en el ejercicio sus atribuciones un total de 142 sistemas de tratamiento de datos personales

- 23 Sistemas por parte de la Unidad de Apoyo Administrativo

- Contrato de Arrendamiento de Inmuebles
- Control de Personal
- Formato Bitácora consumo de Combustible
- Formato de Inventario Vehicular para Automóvil y/o Motocicleta
- Formato de Justificación de Incidencias
- Lista de Asistencia
- Lista de Asistencia a Eventos Formativos
- Lista de asistencia de prestadores de servicio social y/o prácticas profesionales
- Listado de Aceptación de los Instrumentos Normativos en Materia de Ética
- Mantenimiento o Reparación del Mobiliario y Equipo
- Proceso Licitatorio
- Resguardos Provisionales de Mobiliario y Equipo
- Resguardos vehiculares.
- Servicios de Alimentación para Trabajadores de la Secretaría de Hacienda que laboran en horarios extraordinarios
- Solicitud de Evaluación de Personal
- Solicitud de pago a pensionados
- Solicitud de pago a proveedores
- Solicitud de pago de viático y pasaje
- Solicitud de pagos de funerales y defunciones
- Transferencias o bajas del mobiliario y equipo
- CEPCI- Constancia de Compromiso de Aceptación de Cumplimento de los Instrumentos Normativos en Materia de Ética.

- CEPCI- Denuncias ante el Comité de Ética y de Prevención de Conflictos de Interés.
- CEPCI- Listado de Aceptación de los Instrumentos Normativos en Materia de Ética.

06 Sistemas de la Unidad de Archivo

- Capacitación
- Destino Final de las Series (expedientes) documentales
- Existencia de Series (expedientes) documentales
- Ficha Técnica de Valoración Documental
- Préstamo de Expedientes
- Visitantes al Archivo de Concentración

07 Sistemas de la Unidad de Informática

- Bitácora de entrada y salida
- Cuentas de Usuarios en los Sistemas Informáticos
- Emisión de nóminas
- Generación de cuentas de usuarios en los sistemas informáticos normativos
- Servicios Técnicos a Equipos de Cómputo y Periféricos
- Solicitud de Cuentas de Usuarios
- Solicitud de Servicios

02 Sistemas de la Unidad de Inteligencia Económica y Patrimonial

- Lista de Asistencia
- Registro de Visitantes

04 Sistemas de la Unidad de Planeación

- Agenda de Funciones del Servidor Público
- Registro de Asesorías
- Registro de Asistencia para la Coordinación de Grupos de Trabajo
- Responsiva del Sistema Administrador de Formatos

05 Sistemas de la Unidad Técnica

- Asesoría e Información
- Lista de Asistencia
- Proceso de calificación crediticia de las finanzas estatales
- Recepción de correspondencia - Oficialía de Partes
- Registro LI Reunión Nacional de Funcionarios Fiscales

09 Sistemas de la Unidad de Transparencia

- Acreditación de la identidad para el ejercicio ARCO, en su modalidad virtual
- Acta de inspección
- Asistencia y Asesoría
- Bitácora de Vulneraciones
- Comunicados de Carácter Interno
- Generador de Avisos de Privacidad
- Registro de asistencia a cursos de capacitación
- Trámite de solicitudes de acceso a la Información y/o Acceso, Rectificación, Cancelación y Oposición (ARCO) en materia de datos personales

- Inventario de Datos Personales

01 Sistemas de la Unidad de Vinculación de Atención a Auditorías

- Actas Administrativas de Inicio o Cierre y Auditorias, o en su caso determinación de responsabilidades

02 Sistemas de la Unidad de Coordinación Administrativa de Organismos Públicos

- Cuestionario de Funciones
- Registro de asistencia a reuniones

25 Sistemas de la Coordinación General de Recursos Humanos

- Aplicación de evaluación a aspirantes de nuevo ingreso y servidores públicos a la Administración Pública Estatal
- Aplicación de evaluación a servidores públicos de nuevo ingreso a la Administración Pública Estatal
- Atención y/o Asesorías por Gestiones Administrativas y/o Educativas
- Asesoría para la adecuación de estructura orgánica y plantilla de plazas
- Asesoría para la elaboración y actualización de Reglamentos Interiores y Manuales Administrativos
- Bitácora de Acceso
- Constancia de antigüedad laboral
- Constancia de conclusión de asesorías para la elaboración y actualización de Reglamentos Interiores y Manuales Administrativos
- Constancia de sueldos
- Constancia de Sueldo para el Sector Educativo
- Constancia de sueldos para el sector burocracia
- Copias simples o certificadas de documentos
- Descuentos aplicados vía nómina a los servidores públicos
- Descuentos vía nómina por pensión alimenticia
- Expedición de CFDI de Nómina a los Servidores públicos de la Administración de los Organismos Públicos
- Licencias laborales
- Lista de asistencia
- Pago del complemento nominal a la Pensión por Vejez
- Pago de marcha y funeral
- Pensiones
- Sistema de Evaluación de Desempeño (SIED)
- Solicitud de carta de descuento
- Solicitud de constancia de liquidez para la adquisición de vivienda
- Solicitud de Servicios al Sistema de Nómina del Estado de Chiapas NECH
- Usuario y Contraseña para acceso al Sistema Integral de Evaluación del Desempeño (SIED)

04 Sistemas de la Procuraduría Fiscal

- Expedientes de Prescripciones
- Cédulas de Notificación/Fianzas
- Cédulas de notificación/recursos
- Directorio de Control de Visitas al Procurador

08 Sistemas de la Subsecretaría de Egresos

- Cuestionario de Diagnóstico de Necesidades de Capacitación
- Directorio de Enlaces del Sistema de Evaluaciones de la Armonización Contable (SEvAC)

- Directorio del Consejo de Armonización Contable del Estado de Chiapas (CACE)
- Directorio de Enlaces de Seguimiento de las Adecuaciones Presupuestarias del Gasto de Inversión
- Formato de acciones de mejora de los elementos programáticos
- Formato de Directorio Grupo Estratégicos
- Registro a Cursos de Capacitación Sobre el Uso y Manejo de los Sistemas Denominados; SIAHE Fideicomisos Públicos Estatales y SIAHE AC
- Responsiva Entrega de Cuenta Administrador

35 Sistemas de la Subsecretaría de Ingresos

- Alta de vehículos del servicio privado o público.
- Alta de vehículos del servicio privado o público para menores de edad
- Alta y pago del impuesto estatal sobre tenencia de automóviles del servicio público federal por rezagos del año 2015 y anteriores.
- Asesoría Fiscal.
- Aviso para Presentar Dictamen Fiscal e Información Adicional para Sustitución de Contador Registrado
- Baja de placas o reposición de tarjetas de circulación del servicio público o privado
- Cambio de domicilio fiscal del establecimiento mutuante
- Cambio de giro y o domicilio de establecimientos que expenden bebidas alcohólicas.
- Canje de placas o refrendo de tarjetas de circulación del servicio privado o público
- Canje de placas o refrendo de tarjetas de circulación por flotilla del servicio Privado o Público
- Certificación de pago de impuestos estatales y federales coordinados
- Cierre o baja del establecimiento autorizado para la venta de bebidas alcohólicas
- Compensaciones de Contribuciones Estatales y Federales Coordinados
- Constancia de antigüedad de licencias de conducir
- Constancias de no adeudos fiscales
- Convenio de Pago a plazos de créditos fiscales federales y estatales
- Devoluciones de contribuciones estatales y federales coordinados
- Emplacamiento de automóviles, camiones y autobuses del Servicio Privado que trasladen o sean conducidos por personas discapacitadas
- Expedición del permiso para la instalación y funcionamiento de establecimientos mutuantes
- Expedición, Reexpedición y Reposición de licencias de conducir
- Formulario de Registro de Datos para Emisión de CFDI
- Información requerida durante una auditoría federal o estatal
- Inscripción al Registro de Contadores Públicos
- Inscripción al Registro Estatal de Contribuyentes para el pago del derecho de bebidas alcohólicas
- Inscripción y Avisos al Registro Estatal de Contribuyentes
- Modificación y/o reposición de la licencia de funcionamiento para la venta de bebidas alcohólicas
- Pago de Derechos
- Portal de Descarga de Comprobante Fiscal Digital por Internet (CFDI)
- Registro de establecimientos que tengan como actividad la venta de bebidas alcohólicas.
- Revalidación del permiso de instalación y funcionamiento de establecimientos mutuantes
- Registro en el Sistema de Remates
- Sistema de Video-vigilancia de las Áreas de Recaudación
- Solicitud de beneficios fiscales (Condonaciones estatales o federales)
- Sustitución de vehículos del servicio público local
- Trámites y Servicios de la Subsecretaría de Ingresos

03 Sistemas de la Subsecretaría de Planeación

- Asesorías
- Directorio Telefónico
- Lista de Asistencia

- 08 Sistemas de la Tesorería Única

- Bloqueo de Cheques
- Control de Acceso a las Instalaciones de la Tesorería Única
- Control Interno de Entrega de Comprobantes de Transferencia Electrónica
- Entrega de Cheques Nominativos al Beneficiario o Servidor Público Habilitado
- Entrega y Recepción de Recibos Oficiales
- Liberación de Pagos de Sueldos
- Nombramientos de Habilitados para la entrega de Nóminas
- Ordenes de Pagos de Proveedores y Contratistas

A continuación se pone a la vista el formato que se denomina Inventario de datos personales, el cual contiene las siguientes columnas, en las cuales se solicitan a las áreas plasmen los siguientes requerimientos, los cuales se solicitan en cumplimiento a los artículos 50 y 51 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas:

- Nombre del Sistema
- Responsable de Sistema
- Medios de almacenamiento
- Medidas de seguridad
- Forma de obtención
- Catálogo de datos personales
- Servidores públicos que tratan datos personales
- Funciones de los servidores públicos que tratan datos personales
- Identificación de comunicación de datos personales: al interior de la Secretaría, por Transferencia, intervención de encargados
- Ciclo de vida
- Nivel de seguridad.

Nombre del Sistema:_____ **Órgano Administrativo:**_____

Responsable de Siste

	Medios de almacenamiento				**Medidas de seguridad**
Órgano Administrativo	**Físicos**	**Electrónicos**	**Sonoros**	**Otro (s)**	
Unidad de Transparencia	Carpetas Archivos Agendas personales Expedientes	Sistemas:GAP Correos electrónicos personales Correos electrónicos institucionales Nube Base de datos excel Base de datos word			[redacted]

ORMA DE OBTENCIÓN

☐	Presencial	☐	Electrónico
☐	Telefónica	☐	Formalfescrito
☐	electrónico	☐	Transferencias

Firma del enlace

Firma del Responsable de Sistema:

Eliminado la información referente a los resultados obtenidos en los niveles de riesgo identificado, el análisis de riesgo y de brecha, así como las medidas de seguridad existentes e implementadas, por actualizarse la hipótesis normativa prevista en el artículo 136 fracciones V y VII, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas, en correlación con Vigésimo Tercero y Vigésimo Sexto de los Lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

4. ENLISTAR A LOS SERVIDORES PÚBLICOS QUE TRATAN DATOS PERSONALES, ASÍ COMO LOS DATOS REQUERIDOS

Servidores públicos que tienen acceso al tratamiento de los datos personales	Nombre	Cargo	Funciones en materia de protección de datos personales
Unidad de Transparencia			

5	5. A quienes o a que área de les comunican los datos personales al interior de la Secretaría	No aplica
6	Intervienen encargados	☐ SÍ ☐ NO

5. EN CASO DE REALIZAR TRANSFERENCIAS, LLENAR LOS SIGUIENTES CAMPOS.

¿Realiza transferencias? si [ ] no [ ]

Instrumento jurídico con el que se formaliza la prestación de servicio	No aplica
Fecha de Instrumento contractual	No aplica
Finalidad	No aplica

6 **CICLO DE VIDA:**

7. NIVEL DE SEGURIDAD

[redacted]

Funciones y obligaciones de las personas que traten datos personales

De conformidad con el artículo 3, fracción XXIII de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, los servidores públicos de la Secretaría de Hacienda que tratan datos personales en el ejercicio de sus funciones y de las atribuciones de la Unidad Administrativa a la que se encuentran adscritos observan, al menos, las medidas de seguridad técnicas siguientes:

a) Prevenir que el acceso a las bases de datos o a la información, 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) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Adicionalmente, los servidores públicos de la Secretaría de Hacienda, al tratar los datos personales, observarán las siguientes funciones y obligaciones:

Eliminado la información referente a los resultados obtenidos en los niveles de riesgo identificado, el análisis de riesgo y de brecha, así como las medidas de seguridad existentes e implementadas, por actualizarse la hipótesis normativa prevista en el artículo 136 fracciones V y VII, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas, en correlación con Vigésimo Tercero y Vigésimo Sexto de los Lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

Funciones:

¬ Resguardar los datos personales a los que tengan acceso en el ejercicio de sus atribuciones.

¬ Verificar y actualizar el inventario de datos personales de los sistemas de tratamiento de los mismos, a los que tienen acceso.

¬ Llevar un registro de los servidores públicos que accedan a los datos personales y llevar a cabo las acciones necesarias para que sea necesaria la autenticación de los usuarios.

¬ Mantener actualizada la relación de usuarios que traten datos personales.

¬ En caso de que se presente algún incidente de vulneración de seguridad de los datos personales y/o de los sistemas de tratamiento de los mismos, informar dicho incidente a la Unidad de Transparencia de la Secretaría de Hacienda y llevar el registro de los hechos.

Obligaciones:

- Llevar a cabo permanentemente las medidas de seguridad de carácter administrativo, físico y técnico necesarias para la protección de los datos personales, evitando daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado, así como garantizando la confidencialidad, integridad y disponibilidad de los mismos.

- Atender los mecanismos para asegurar que los datos personales a los que tengan acceso en el ejercicio de sus atribuciones no se difundan, distribuyan o comercialicen.

Por otra parte, el formato denominado inventario de datos personales y de los sistemas de tratamiento o bases de datos personales contiene las siguientes columnas, en las cuales se identifican las funciones del personal que interviene en

el tratamiento de los datos personales:

4. ENLISTAR A LOS SERVIDORES PÚBLICOS QUE TRATAN DATOS PERSONALES, ASÍ COMO LOS DATOS REQUERIDOS

Servidores públicos que tienen acceso al tratamiento de los datos personales	Nombre	Cargo	Funciones en materia de protección de datos personales
Unidad de Transparencia	[illegible]	[illegible]	[illegible]

5	5. A quienes o a que área de les comunican los datos personales al interior de la Secretaría	No aplica
6	Intervienen encargados	☐ SÍ ☐ NO

Inventario de Datos Personales y de los sistemas de Tratamiento

En cumplimiento a lo establecido en los artículos 33, fracción III y 35, fracción I de la Ley General de Datos Personales en Posesión de Sujetos Obligados, esta Secretaría de Hacienda, con la finalidad de establecer y mantener las medidas de seguridad para la protección de los datos personales, emitió el presente inventario de datos personales y de los sistemas de tratamiento, con la información básica del tratamiento de datos personales señalado por las Unidades Administrativas de esta Secretaría.

De igual forma para cumplir con los objetivos y obligaciones que prevé la LGPDPPSO, particularmente en materia de seguridad y, como parte del Sistema de Gestión de Seguridad de Datos Personales de la Secretaría Hacienda, se identificaron los procesos que se llevan a cabo para el tratamiento de datos personales; obteniendo con ello el denominado Inventario de Datos Personales de la Secretaría de Hacienda. Por inventario de tratamiento de datos, se entiende el control documentado del conjunto de operaciones que realizan las áreas que integran la Secretaría de Hacienda con motivo de los datos que se recaban de las personas y/o titulares, 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. En tal virtud, en coordinación con las áreas y derivado del proceso de actualización de información, se advirtió que, en general las unidades administrativas que conforman la estructura orgánica de la institución llevan a cabo el tratamiento de datos personales.

Las áreas que forman parte de esta Secretaría de Hacienda y que deberán observar el programa, son las siguientes:

- Unidad de Apoyo Administrativo
- Unidad de Archivo
- Unidad de Informática
- Unidad de Inteligencia Patrimonial y Económica
- Unidad de Planeación
- Unidad Técnica
- Unidad de Transparencia
- Unidad de Vinculación de Atención a Auditorías
- Unidad de Coordinación Administrativa de Organismos Públicos
- Coordinación General de Recursos Humanos
- Procuraduría Fiscal
- Subsecretaría de Egresos
- Subsecretaría de Ingresos
- Subsecretaría de Planeación
- Tesorería Única

Por inventario de datos personales se entenderá el control documentado que se llevará de los tratamientos que realizan las áreas de la Secretaría de Hacienda, realizado con orden y precisión.

Sobre el particular, los artículos 53 y 54 de los Lineamientos establecen lo siguiente:

Inventario de datos personales.

Artículo 53.- Con relación a lo previsto en el artículo 47, fracción III, de la Ley Estatal, el responsable deberá elaborar un inventario con la información básica de cada tratamiento de datos personales, considerando, al menos, los siguientes elementos: I. El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales; II. Las finalidades de cada tratamiento de datos personales; III. El catálogo de los tipos de datos personales que se traten, indicando si son

sensibles o no; IV. El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales; V. La lista de servidores públicos que tienen acceso a los sistemas de tratamiento; VI. En su caso, el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable, y VII. En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican éstas. Ciclo de vida de los datos personales en el inventario de éstos.

Artículo 54.- Aunado a lo dispuesto en el artículo anterior de los presentes Lineamientos, en la elaboración del inventario de datos personales el responsable deberá considerar el ciclo de vida de los datos personales conforme lo siguiente: I. La obtención de los datos personales; II. El almacenamiento de los datos personales; III. El uso de los datos personales conforme a su acceso, manejo, (SIC) IV. Aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin; (SIC) V. La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen; VI. El bloqueo de los datos personales, en su caso, y VII. La cancelación, supresión o destrucción de los datos personales. A partir de lo anterior, la Secretaría de Hacienda elaboró los inventarios de los distintos tratamientos de datos personales que realizan o efectúan sus áreas, identificando la mayor parte de los elementos informativos que prevén los artículos 50 de la LPDPPSOCHIS y 53 de los Lineamientos, basado en el ciclo de vida de los datos personales, tal como lo requiere el artículo 54 de dichos Lineamientos.

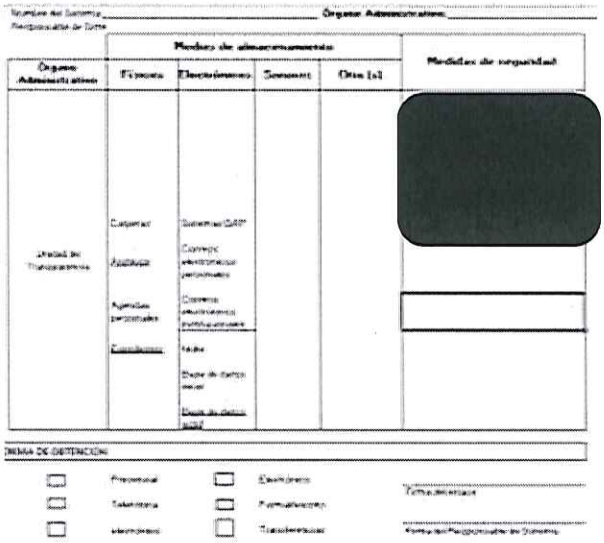
A partir de lo anterior, la Secretaría de Hacienda elaboró los inventarios de los distintos tratamientos de datos personales que realizan o efectúan sus áreas, identificando la mayor parte de los elementos informativos que prevén los artículos 50 de la LPDPPSOCHIS y 53 de los Lineamientos, basado en el ciclo de vida de los datos personales, tal como lo requiere el artículo 54 de dichos Lineamientos.

Asimismo, durante el proceso de sistematización se observó que los datos personales cuyo tratamiento se lleva a cabo en los 142 Sistemas de datos personales, corresponden a las siguientes 7 categorías de datos personales:

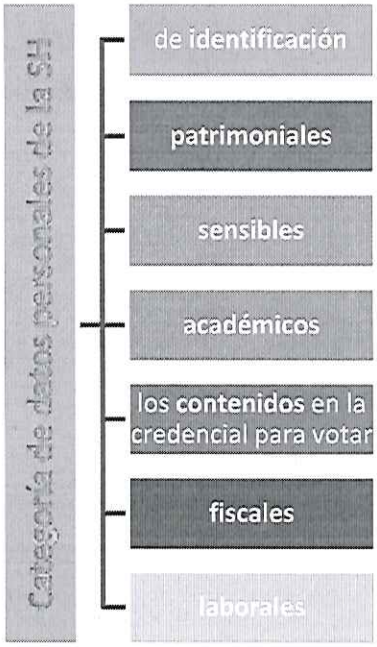
Tipo de dato personal	Nivel de riesgo inherente	Volumen de titulares				
		<500	<5k	<50k	<500k	>500k
Datos de Identificación	Bajo	1	1	1	1	1
Electrónicos	Bajo	1	1	1	1	1
Académicos	Bajo	1	1	1	1	1
Laborales	Bajo	1	1	1	1	1
De relaciones profesionales	Bajo	1	1	1	1	1
Fiscales	Medio	1	1	2	3	3
De relaciones comerciales	Medio	1	1	2	3	3
Sobre procedimientos administrativos y/o jurisdiccionales	Medio	1	1	2	3	3
Patrimoniales	Medio	1	1	2	3	3
Afectivos y/o familiares	Alto	2	2	3	3	3
Sobre movimientos migratorios	Alto	2	2	3	3	3
Sensibles	Alto	2	2	3	3	3
De salud	Alto	2	2	3	3	3
Menores	Alto Reforzado	4	4	5	5	5
Ubicación o domicilio particular en conjunto con datos de nivel medio o alto	Alto Reforzado	4	4	5	5	5

Simbología: < igual o menor a; > igual o mayor a; k es igual a mil o miles.

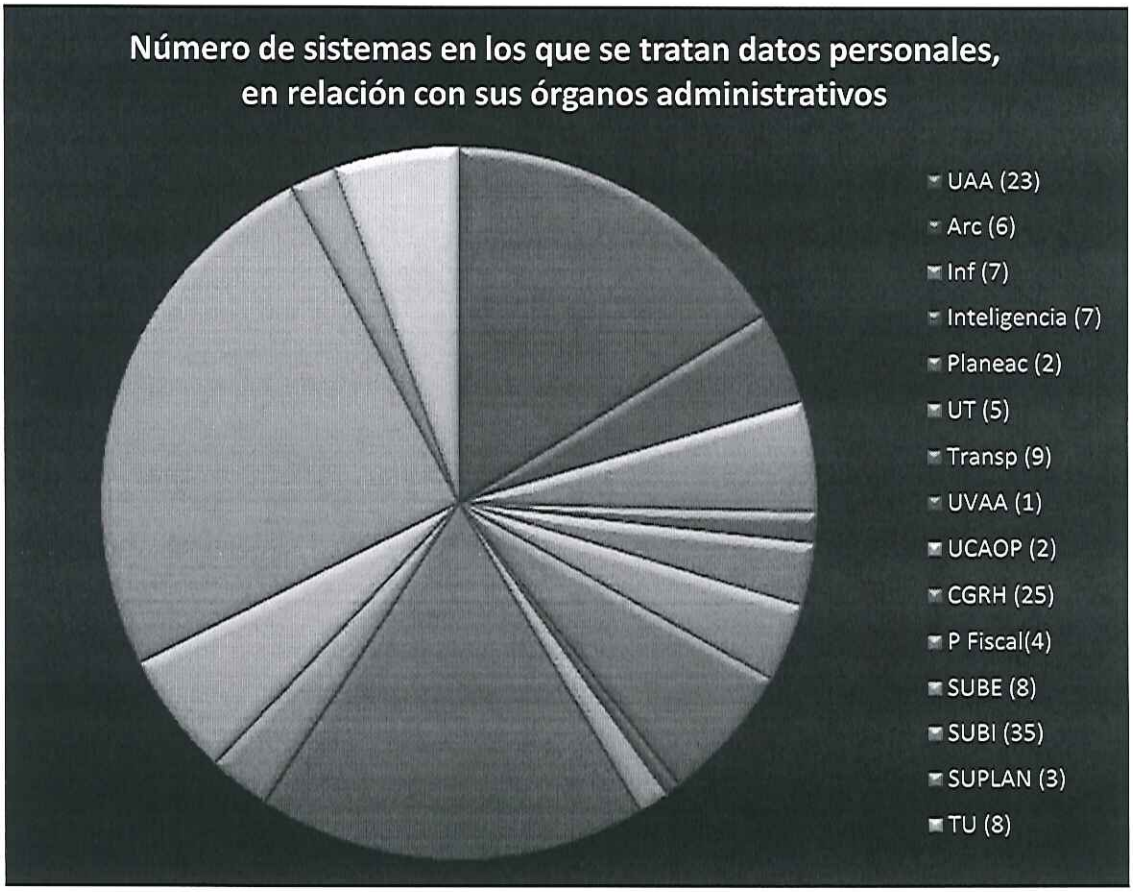
Por otra parte, el formato denominado inventario de datos personales y de los sistemas de tratamiento o bases de datos personales contiene las siguientes columnas, en las cuales se identifican las funciones del personal que interviene en el tratamiento de los datos personales:



Eliminado la información referente a los resultados obtenidos en los niveles de riesgo identificado, el análisis de riesgo y de brecha, así como las medidas de seguridad existentes e implementadas, por actualizarse la hipótesis normativa prevista en el artículo 136 fracciones V y VII, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas, en correlación con Vigésimo Tercero y Vigésimo Sexto de los Lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.


Categoría de datos personales de la su
de identificación
patrimoniales
sensibles
académicos
los contenidos en la credencial para votar
fiscales
laborales

A continuación, se presenta de manera gráfica la distribución de los sistemas de datos personales que se tratan en la Secretaría de Hacienda de acuerdo a los órganos que la conforman:



Se puede observar en la gráfica anterior a los órganos administrativos de la Secretaría de Hacienda que poseen el mayor número de operaciones en las que intervienen tratamientos de datos personales, dada la naturaleza de sus funciones, toda vez que entre las áreas que la integran se encuentran aquellas con atribuciones para administrar los recursos humanos, materiales y financieros de la institución, por lo que el hallazgo en sí mismo representa un insumo imprescindible para el cumplimiento de sus funciones. Por tal motivo, las áreas de atención, oportunidad y verificación en materia de protección de datos deben contar con un enfoque de importancia en el desarrollo de las actividades de esta unidad administrativa.

Debe destacarse que, si bien la Unidad de Apoyo Administrativo y la Coordinación General de Recursos Humanos son las áreas administrativas con más

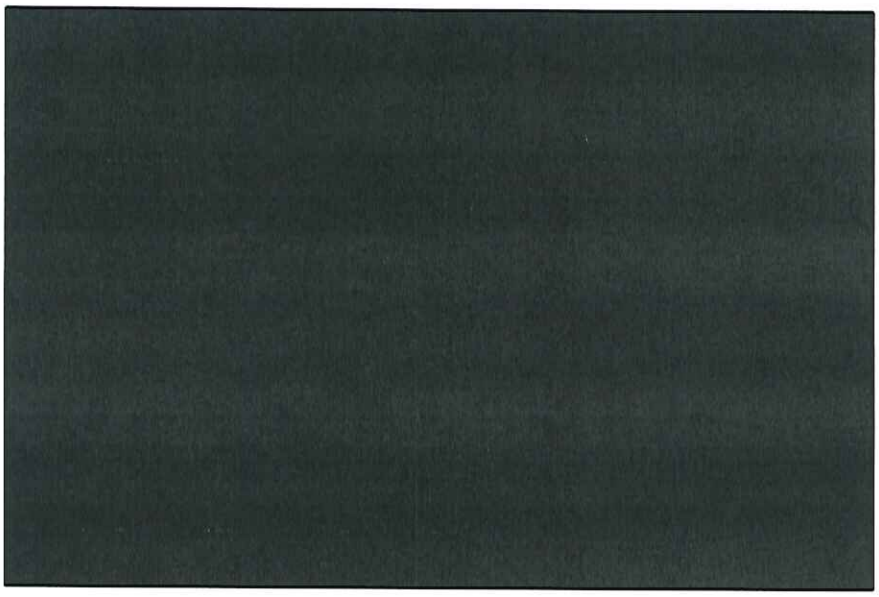
operaciones en las que convergen el tratamiento de datos, también lo es que todas las demás, en menor medida, por lo que la política de protección debe ser entendida como una acción de frecuencia generalizada.

Ante este contexto, es dable concluir que el Inventario de Datos Personales de la Secretaría de Hacienda, a partir de los hallazgos identificados, se constituye como un elemento del Sistema de Gestión de Datos Personales, que junto con las medidas de seguridad representa un instrumento de evidencia de la implementación de las directrices de la Política en materia de protección de datos personales.

VIII Accesos Controlados y Bitácoras

La Secretaría de Hacienda, implementa las bitácoras de acceso para prevenir intromisiones o los accesos no autorizados a las áreas, permitiendo solo al personal previamente identificado.

A continuación se presentan como evidencia documental, las áreas de la Secretaría de Hacienda que decidieron implementar como una medida de seguridad las bitácoras de acceso.



IX y X Análisis de riesgos y de brecha

El presente análisis identifica el riesgo inherente a los datos personales en el tratamiento que reciben por la de Hacienda al ejercer sus atribuciones, de manera que pueda ser controlado por la institución para satisfacer el derecho humano a la autodeterminación informativa. La LGPDPPSO en sus artículos 32, fracción I, y 33, fracción IV, considera que el determinar el riesgo inherente a los

Eliminado la información referente a los resultados obtenidos en los niveles de riesgo identificado, el análisis de riesgo y de brecha, así como las medidas de seguridad existentes e implementadas, por actualizarse la hipótesis normativa prevista en el artículo 136 fracciones V y VII, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas, en correlación con Vigésimo Tercero y Vigésimo Sexto de los Lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

datos personales tratados es un deber de los sujetos obligados en la adopción de medidas de seguridad, para lo que debe realizar un análisis que considere las amenazas y vulnerabilidades para los datos, así como los recursos involucrados en el tratamiento.

Con base en la LGPDPPSO, la valoración de los riesgos de los datos personales forma parte de los elementos mínimos que contiene este instrumento que describe y da cuenta, en lo general, sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas (Documento de seguridad), en este caso, por la Secretaría de Hacienda, con el propósito de garantizar la confidencialidad, integridad y disponibilidad de ese tipo de datos bajo su posesión.

Los datos personales a los que los servidores públicos de esta Secretaría tienen acceso en el ejercicio de sus atribuciones, se resguardan de manera física y electrónica, según las necesidades de la actividad para la cual se lleva a cabo su tratamiento. Tanto para la protección de datos personales, como para los datos personales sensibles, determinados junto con su ciclo de vida por las Unidades Administrativas en el "Inventario de Datos Personales" la Secretaría de Hacienda observa el máximo nivel de protección; es decir, sin discriminarlos por su valor o ciclo de vida, pues su vulneración podría tener como consecuencia negativa para los titulares de los datos personales la divulgación o incluso un daño en su esfera más íntima, daño moral o patrimonial, entre otros, siendo que el valor de los datos personales en la actualidad cobra cada día mayor relevancia por las implicaciones e información vinculados a ellos.

En este sentido, tanto los sistemas electrónicos como los medios a través de los cuales se resguardan de manera física los datos personales presentan diferentes particularidades en razón de las características de cada uno de ellos y de las medidas físicas inherentes a los servicios que presta la Secretaría de Hacienda, ya que cuanta con Delegaciones y Centros de Recaudación Local en diversas parte del Estado. Por lo que hace a los datos personales que se resguardan de manera física, esta Secretaría ha contemplado los riesgos futuros los cuales pueden consistir en la pérdida o uso indebido de la información, deterioro negligente, así como su destrucción; por ello, la Secretaría de Hacienda en sus diversas delegaciones cuenta con un área soporte encargada de ejecutar acciones para garantizar la seguridad de la información, manteniendo en un mínimo su exposición, pues únicamente pueden acceder a ellos los servidores públicos facultados y con acreditación para su uso.

Por su parte, los datos personales contenidos en un sistema electrónico presentan riesgos por su propia naturaleza como lo son el uso indebido de la información, la falla en los equipos electrónicos o en los sistemas; por ello, la Secretaría de

Hacienda cuenta con un área soporte encargada de ejecutar acciones para garantizar la seguridad de la información, manteniendo en un mínimo su exposición, pues únicamente pueden acceder a ellos los servidores públicos facultados y previa acreditación de su personalidad a través de medios electrónicos para su uso.

Para la determinación del riesgo sobre esa tipología de datos personales se valora la probabilidad e impacto de que, en su obtención, almacenamiento, tratamiento, transferencia o remisión, bloqueo y/o eliminación (ciclo de vida), en correspondencia con una diversidad de activos involucrados, se materialice uno o más factores que pueden causar un daño a su titular (amenaza). Para facilitar el análisis, se establecieron cuatro tipos de amenazas:

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

Por otra parte, el formato denominado análisis de riesgo y brecha contiene las siguientes columnas, en las cuales se identifican los riesgos en el tratamiento de los datos personales:

- Órgano Administrativo
- Denominación (nombre) del tratamiento o proceso
- Fundamento jurídico que habilita el tratamiento
- Atribuciones, facultades y/o funciones para realizar el tratamiento
- No. de Tratamientos
- Tipo de Datos Personales
- Datos sensibles
- Tipo de Datos Sensibles
- Tipos de Amenzas
- Ciclo de vida de acuerdo a la dispoición legal que le aplique
- Probabilidad del nivel de amenaza en las distintas etapas de vida de los Datos Personales (Nivel de riesgo)
- Consecuencia desfavorable (impacto)

Eliminado la información referente a los resultados obtenidos en los niveles de riesgo identificado, el análisis de riesgo y de brecha, así como las medidas de seguridad existentes e implementadas, por actualizarse la hipótesis normativa prevista en el artículo 136 fracciones V y VII, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas, en correlación con Vigésimo Tercero y Vigésimo Sexto de los Lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

XI Gestión de Vulneraciones

En la medida en que los titulares de sus datos personales estén preparados para afrontar una vulneración podrán responder de forma rápida, ordenada y eficaz (capacidad de respuesta) ante dicha situación, minimizando las consecuencias tanto para los titulares como para el Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Chiapas por lo que se sugiere que las áreas que traten datos personales:

Dispongan de un Plan de respuesta a incidentes. Es recomendable y, en algunos casos obligatorio dependiendo del tipo, cantidad de datos personales tratados, número de titulares y riesgos de privacidad identificados- que las áreas propietarias cuenten con procedimientos o planes de actuación denominados Planes de respuesta a incidentes. Estos planes incluyen, entre otros puntos, la forma de detectar las alertas de seguridad para determinar si se trata de un incidente, así como las especificaciones sobre las herramientas y equipo a utilizar para su atención. Lo anterior también aplica a los Encargados, para permitir un tratamiento adecuado de los datos personales y una comunicación apropiada con los responsables.

La Secretaría de Hacienda cuanta con un formato publicado en la página web de esta denominado Bitácora de vulneraciones, mismo que será utilizado en el caso de que ocurra alguna vulneración y se pueda dar atención inmediata a esta, a través de la Unidad de Transparencia.

http://www.haciendachiapas.gob.mx/SitioNuevo/TramitesHacienda

Para gestionar las vulneraciones es necesario que el área propietaria identifique claramente a las personas que estarán involucradas, mediante las siguientes actividades:

- Determinar los medios para comunicar las vulneraciones. Este paso es importante para establecer una eficiente comunicación entre el personal que designado para su atención.

- Para confirmar la vulneración, realizar lo siguiente:

Si, el área propietaria entonces, debe:

a) Detectar una ejecución inadecuada de los procedimientos establecidos o sistemas informáticos que tratan datos personales provocando interrupción o desvío que pudiera afectar su seguridad.

b) Recibe una notificación de un incidente de seguridad de la información que afecta sus procesos de negocio.

SECRETARÍA DE HACIENDA

BITÁCORA DE VULNERACIONES
IDENTIFICACIÓN DE INCIDENTES

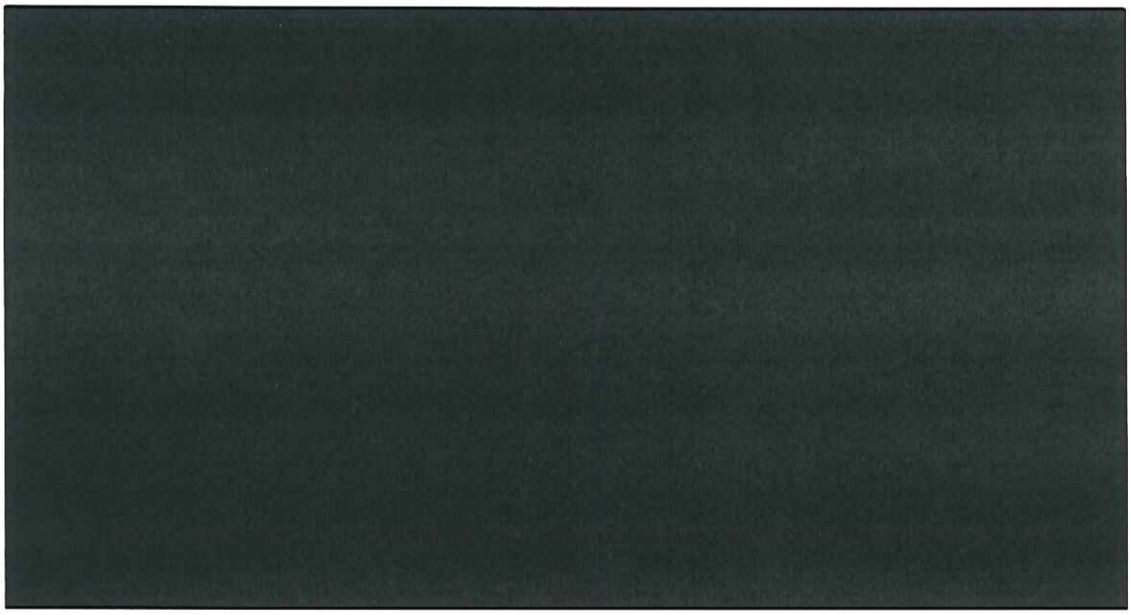
	Fecha del incidente Hora del incidente		Titulares afectados
Organismo administrativo			
Nombre de quien reporta			
Correo electrónico de quien reporta			
Área donde ocurre la vulneración			
Nombre del Sistema comprometido			
TIPO DE SISTEMA DE TRATAMIENTO DE DATOS PERSONALES			
Físico		Electrónico	
NOMBRE DEL RESPONSABLE DEL SISTEMA DE TRATAMIENTO y/o ENCARGADO			IMPACTO DEL INCIDENTE
ENLISTAR DATOS PERSONALES COMPROMETIDOS			
			ACCIONES CORRECTIVAS IMPLEMENTADAS DE MANERA INMEDIATA
DESCRIPCIÓN DE LO SUCEDIDO ¿Como fue detectado?, ¿Que sucedió?, ¿Que lo causó?			

XII Las medidas de seguridad existentes y efectivas implementadas actualmente en la Secretaría de Hacienda para la protección de datos personales con las que actualmente cuenta la Secretaría de Hacienda

1. Medidas de seguridad: La información que contiene datos personales se resguarda en una ubicación que cuenta con diversas medidas de seguridad como cámaras de seguridad, archiveros específicos para su resguardo y uso de cerraduras para su acceso.

2. Medidas de carácter administrativo encaminadas a contar con un registro físico de los servidores públicos que tienen acceso a datos personales, así como de los datos personales contenidos en los documentos.

3. Medidas legales: Cuando se lleva a cabo la transferencia de datos personales entre sujetos obligados o entre servidores públicos de la Secretaría de Hacienda, se realiza el apercibimiento en cuanto al trato que se le deberá dar a los mismos, en los términos de la legislación vigente en la materia.



Se trata de todas aquellas medidas que adopta el Comité de Transparencia de la Secretaría de Hacienda y en su caso, en conjunto con el área que posea los datos personales, siempre que sea necesario para asegurar que la información confidencial y los datos personales sean resguardados de manera íntegra, segura

Eliminado la información referente a los resultados obtenidos en los niveles de riesgo identificado, el análisis de riesgo y de brecha, así como las medidas de seguridad existentes e implementadas, por actualizarse la hipótesis normativa prevista en el artículo 136 fracciones V y VII, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas, en correlación con Vigésimo Tercero y Vigésimo Sexto de los Lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

y adecuada, ya sea a través de mecanismos administrativos, técnicos, físicos, políticas de procesos y controles.

De conformidad con lo señalado por la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, los deberes sobre la Seguridad de los datos personales, se entenderán tal y como lo marca el artículo 45 que a la letra dice:

Artículo 45.- *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.

Dentro de las medidas de seguridad que se tienen señaladas por la Ley de la materia y que deben ser seguidos los elementos que ahí se señalan:

- Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización, formación 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 consideran las siguientes actividades:
    - Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
    - Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;

- Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

- Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
- Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware; y
- Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Por lo tanto, las áreas que integran la Secretaría de Hacienda aplicarán el nivel básico, medio o alto de medidas de seguridad, de acuerdo con la categoría o tipos de datos personales.

1. NIVEL BÁSICO. - Estas medidas serán aplicables a todos los sistemas de datos personales de la Secretaría:

   • De Identificación: Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma (en cuanto ésta no resulta confidencial cuando se emita en cumplimiento de la obligación legal para las funciones que fue contratado el servidor público y deba autorizar la emisión de un documento que por sus actividades resulta necesario para avalar el contenido del texto), firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, fotografía.

   • Labores: Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, actividades extracurriculares, referencias laborales, referencias personales entre otros. La posesión de datos personales deberá obedecer exclusivamente a las atribuciones legales o reglamentarias de cada entidad y deberán obtenerse a través de los medios previstos; estos datos sólo deberán tratarse únicamente para la finalidad para la cual fueron obtenidos. Cuando los datos personales se actualicen no deben de alterar la veracidad de la información que tengan y debe de ser por personal autorizado para el cumplimiento de las atribuciones de esta Secretaría.

2. NIVEL MEDIO. - Los datos personales además de cumplir con las medidas de seguridad de nivel básico:

   • Datos Patrimoniales: Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros.

   • Datos sobre procedimientos administrativos seguidos en forma de juicio y/o jurisdiccionales: Información relativa a una persona que se encuentre

sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa.

• Datos Académicos: Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros.

• Tránsito y movimientos migratorios: Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas entre otros.

Este tipo de datos debido a la trascendencia para la intimidad, se debe evitar prejuicios por el uso que se pueda hacer con ese tipo de información siendo factores de generar graves conflictos, si no tienen el debido cuidado al manejar la información confidencial.

3. NIVEL ALTO. Los datos personales que contengan algún dato que se enliste deberán cumplir con las medidas de seguridad de nivel básico y medio, deberán observar las marcadas con el nivel alto.

• Datos Ideológicos: Creencia religiosa, ideología, filosófica, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y/o asociaciones religiosas, entre otros.

• Datos de Salud: Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, entre otros.

• La ubicación de menores de edad: a través de sus datos académicos y toda la información que se posea de estos, toda vez que la revelación de algún dato personal puede poner en riesgo la integridad de menores.

• Características personales: Tipo de sangre, ADN, huella digital, u otros análogos.
• Características físicas: Color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otras.

• Vida sexual: Preferencia sexual, hábitos sexuales, entre otros.

• Origen: Étnico y racial.

Otras medidas aplicables:

A. Declaración de confidencialidad: realizar esta declaración que será puesta a disposición del personal que interviene en el tratamiento de datos personales para que estén informados de los deberes y medidas de

seguridad que deben tomar en consideración en sus actividades relacionadas con dichos tratamientos.

B. Capacitación: el personal involucrado en el tratamiento de los datos personales deberá asistir a los cursos de capacitación implementados por el Comité de Transparencia en el Programa Anual de Capacitación.

C. Bitácora de vulneraciones: implementar un control informativo en donde se reporten los tipos de vulneraciones1 con los siguientes datos: fecha y lugar en donde se produjo, nombre y cargo de quien notifica la incidencia, nombre y cargo de la persona a la que se le comunica, y las medidas que se implementaron para subsanar la misma. Toda vulneración deberá notificarse, también, a la Unidad de Transparencia para que tome las acciones pertinentes. Si la vulneración trasciende a una posible afectación directa de los titulares de los datos personales, especialmente en sus derechos patrimoniales o en su esfera más íntima (datos sensibles), se deberá notificar a los titulares afectados para que tomen las medidas pertinentes para la defensa de sus derechos.

D. Transferencias: realizar transferencias con las medidas de confidencialidad necesarias, enviar la información en sobre cerrado y con la leyenda de "confidencial" o en archivos electrónicos encriptados.

E. Prevenir accesos no autorizados: prevenir que el acceso a las bases de datos o a la información, así como a los recursos que las contengan, se realice únicamente por usuarios identificados y autorizados por el área.

XVIII Para el tratamiento de datos personales, se considera realizar el monitoreo, bajo las siguientes políticas:

De las políticas internas, relacionadas con el tratamiento de datos personales las cuales tienen el objetivo de asegurar que los servidores públicos que realicen los tratamientos de datos personales derivados de sus facultades y atribuciones, lo hagan en concordancia con el marco normativo del Reglamento Interior de la Secretaría y de las disposiciones de la materia en protección de datos personales. Para ello, cuando se identifica algún cambio en los instrumentos antes mencionados, se deberán realizar las siguientes actividades:

- Revisar y, en su caso, actualizar los procesos involucrados en el tratamiento de datos personales.
- Revisar y, en su caso, actualizar los avisos de privacidad, las funciones y obligaciones del personal y los inventarios de datos personales, según corresponda.
- Evaluar si hubo cambios en las amenazas, vulnerabilidades o impacto de los riesgos relacionados con las modificaciones a la normativa, para actualizar los análisis de riesgos, análisis de brecha y plan de trabajo.
- Revisar y, en su caso, adecuar los sistemas de tratamiento para cumplir con los cambios normativos.

- Revisión del riesgo. Tiene el objetivo de identificar modificaciones a los riesgos identificados en los tratamientos de datos personales, para ello, se implementarán las siguientes acciones:
  - Monitoreos:

    a. Monitoreo del entorno físico. Para la detección continua de amenazas y vulnerabilidades en el entorno físico, se cuenta con:

    (i) control de acceso a través de bitácoras para visitantes, y

    (ii) Video vigilancia en las delegaciones de la Secretaría

- Actualización del plan de trabajo. Derivado del monitoreo del entorno físico, se pueden realizar actualizaciones en el plan de trabajo en caso de que se identifiquen cambios en las amenazas, las vulnerabilidades o el impacto de los riesgos identificados.

- Revisión de avances del plan de trabajo. A través de los mecanismos que determine el área que apoya en el análisis de riesgos, el Comité de Transparencia revisa los avances en el plan de trabajo, identificando las acciones, fechas compromiso y, en su caso, las causas por las cuales no se está cumpliendo el plan de trabajo, para hacer los ajustes correspondientes al mismo.

Mecanismos de supervisión o revisión

Además del monitoreo continuo de las medidas de seguridad, se requiere realizar una supervisión periódica de las medidas de seguridad, a través de auditorías, las cuales pueden ser internas o externas. Hasta el momento no se han realizado auditorías específicas en materia de protección de datos personales. Así, respecto del programa de auditoría, se tiene contemplada la realización de una auditoría en materia de protección de datos personales, al menos una vez al año. El programa de auditoría será aquél que determine el Comité de Transparencia en el Programa de Protección de Datos Personales.

A través de la Unidad de Transparencia, se han llevado a cabo dos auditorías a distintos órganos administrativos de la Secretaría y con distinta objetividad. La primera revisión se llevó a cabo para la constatar que las áreas de la Secretaría cumplían con poner a disposición sus avisos de privacidad. La segunda revisión consistió en revisar aleatoriamente a las Delegaciones de la Secretaría, en las que se constató el conocimiento en la materia de protección de datos personales; la aplicación de las medidas de seguridad físicas, técnicas y administrativas; el uso correcto de las hojas recicladas, la disposición de los avisos de privacidad, el tratamiento adecuado de los datos sensibles y de menores.

XVI TÉCNICAS UTILIZADAS PARA LA SUPRESIÓN Y BORRADO SEGURO DE LOS DATOS PERSONALES

La Ley desarrolla una serie de principios y deberes que establecen obligaciones concretas para los responsables del tratamiento de datos personales, a fin de crear condiciones para la protección de los datos, evitar malos manejos de los mismos, y permitir que las personas ejerzan su derecho a la autodeterminación informativa. Para el caso que nos ocupa, destaca el principio de calidad y el deber de seguridad.

El principio de calidad establece que, conforme a la finalidad o finalidades para las que se vayan a tratar los datos personales, éstos deben ser exactos, completos, pertinentes, actualizados y correctos. Asimismo, este principio señala que cuando los datos personales hayan dejado de ser necesarios para las finalidades para las cuales se obtuvieron, deben ser eliminados, tomando en cuenta las disposiciones legales aplicables para los plazos de conservación. En ese sentido, con independencia de que un titular de los datos personales ejerza su derecho de cancelación, el responsable del tratamiento está obligado a eliminar, de oficio, los datos personales cuando hayan dejado de ser necesarios para la finalidad para la cual se obtuvieron.

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

Por lo anterior, a continuación se presenta la evidencia documental en la que la Secretaría de Hacienda a través de sus órganos da cabal cumplimiento a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas

XVII PLAN DE TRABAJO

En función de las particularidades que revela dicho instrumento, es posible obtener información sobre necesidades específicas de las áreas que integran la Secretaría de Hacienda para el diseño de planes de trabajo; así como la implementación y factibilidad de mecanismos de monitoreo y revisión de medidas de seguridad, que también integran el Documento de Seguridad y son imprescindibles para que el Comité de Transparencia disponga lo conducente en torno a estas medidas institucionales.
Derivado de lo anterior la Unidad de Transparencia perfiló el presente Plan de Trabajo como una herramienta complementaria y de instrumentalización del Documento de Seguridad previamente aprobado por el Comité de Transparencia, cuyos objetivos fundamentales son los siguientes:

1. Eliminar las brechas a través de la implementación de medidas de seguridad pendientes en cada uno de los tratamientos de datos personales identificados; y,

2. Consolidar y preservar los niveles de protección de los datos personales a través de mecanismos de monitoreo y revisión.

   Es necesario advertir sobre la importancia de generar esquemas de trabajo interdependientes con aquellas áreas que juegan un papel trascendental en la protección de los datos personales a nivel institucional y que están involucradas en la generación de las políticas, acciones y medidas que se describen más adelante.

Cronograma 2022

Actividades	Enero 1	Febrero 3	Marzo 1	Abril 1	Mayo 1	Junio 1	Julio 1	Agosto 1	Sep. 1	Oct. 1 2	Nov. 1 2	Diciembre 1 2
Asesorar a las Unidades Administrativas en materia de Datos Personales especificamente respecto de las medidas de seguridad.												
Consultar vía oficial a las distintas áreas que integran la Secretaría de Hacienda, la ratificación de los enlaces en Materia de Datos personales												
Dar a conocer a las áreas que integran a la Secretaría de Hacienda las obligaciones en materia de protección de datos personales conforme lo establecido en la Ley General y la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.												
Dar a conocer vía oficial, las sanciones a todas las áreas que integran la Secretaría de Hacienda y/o traten datos personales, por el incumplimiento a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.												
Para el debido cumplimiento de las obligaciones en materia de Datos Personales, vía oficial, se le requerirá a cada una de las unidades administrativas que integran la Secretaría de Hacienda realicen un diagnóstico respecto al análisis de riesgos y análisis de brecha												
Capacitación Integral en materia de protección de datos personales												
Capacitación y/o sensibilización respecto a las Medidas de seguridad físicas y técnicas de los datos personales así como darles a conocer el Plan de Trabajo en materia de protección de datos personales.												
Realizar auditorías internas a las áreas que integran la Secretaría, para comprobar el cumplimiento de las políticas de protección de datos personales												
Solicitar a las áreas, con el afán de verificar las medidas de seguridad de carácter físico, técnico y administrativo, los documentos que avalen tal cumplimiento.												
Requerirles a las oficinas que integran la Secretaría de Hacienda las bitácoras de las vulneraciones a la seguridad.												
Enviar a las áreas vía oficial el instrumento jurídico mediante el cual formalizan la relación de encargado y responsable con la finalidad que se empiecen los trabajos de actualización del documento de seguridad.												
Presentar un Informe anual al titular de la Institución, en el que describan las acciones realizadas para el cumplimiento de las obligaciones en materia de Datos Personales												