DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE LOS DATOS PERSONALES EN POSESIÓN DE LA OFICIALÍA MAYOR DEL ESTADO DE CHIAPAS

Introducción

El derecho a la protección de los datos personales es un derecho humano reconocido en la Constitución Política de los Estados Unidos Mexicanos en sus artículos 6, apartado A, fracción II y 16, párrafo segundo; su regulación específica para el sector público es la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la cual fue publicada el 26 de enero de 2017 en el Diario Oficial de la Federación (DOF).

La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, define los datos personales como cualquier información concerniente a una persona física identificada o identificable, por lo que se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información; por otra parte, hace la distinción entre los datos personales sensibles, los cuales se definen como aquellos que se refieren a la esfera más íntima de su titular, cuya utilización indebida pueda dar origen a discriminación o conllevé un riesgo grave para este, para enunciar algunos se consideran sensibles los datos que revelan aspectos como origen racial o étnico, estado de salud pasado, presente o futuro, creencias religiosas, filosóficas y morales, opiniones políticas, datos genéticos, datos biométricos y preferencia sexual; de conformidad con lo dispuesto en el artículo 5, fracción XIII de dicha legislación, un Documento de Seguridad es el Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad de carácter técnico, físico y administrativo adoptadas por el responsable, para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

De conformidad con lo dispuesto en el artículo 4 del Decreto por el que se crea la Oficialía Mayor del Estado de Chiapas, publicado en el Periódico Oficial número 006, Tomo III, Quinta Sección, de fecha 31 de diciembre de 2018, reformado mediante Decreto publicado en el Periódico Oficial número 202, Tomo III, de fecha 31 de diciembre de 2021, la Oficialía Mayor tiene como objeto fundamental, la ejecución de la política relacionada con la administración de los recursos materiales y servicios, fungiendo como área consolidadora de los procedimientos de compra de bienes y contratación de servicios que se determinen, con base en la legislación aplicable.

Por lo anterior, este Órgano Desconcentrado, con la finalidad de establecer y mantener las medidas de seguridad 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, para el tratamiento de los datos personales en el ejercicio de sus atribuciones.

Objetivo del documento de seguridad.

El presente documento tiene como objetivo establecer y controlar internamente:

- El tratamiento de datos personales en posesión de la Oficialía Mayor.
- Los datos personales que integran los archivos.
- Las obligaciones de los responsables del tratamiento de la información.
- El análisis de los posibles riesgos que pudieran enfrentar los órganos administrativos de este Sujeto Obligado en el ejercicio de sus atribuciones.
- Los mecanismos de monitoreo y la revisión de las medidas de seguridad.

En cumplimiento a lo establecido en los artículos 45, 49 y 50 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, esta Oficialía Mayor con la finalidad de implementar y mantener las medidas de seguridad para la protección de los datos

personales, emite la siguiente información básica del tratamiento de datos personales señalado por los Órganos Administrativos de este Sujeto Obligado.

I. Nombres de los sistemas de tratamiento.

Los datos personales en posesión de la Oficialía Mayor del estado de Chiapas son sometidos a los siguientes tratamientos:

1. Registro de audiencias de la oficina del C. Oficial Mayor.
2. Control de la agenda del C. Oficial Mayor.
3. Integración y resguardo de los expedientes laborales de los Servidores Públicos de la Oficialía Mayor del Estado de Chiapas.
4. Integración y resguardo de las nóminas de pago de los servidores públicos de la Oficialía Mayor del Estado de Chiapas.
5. Integración y resguardo de la hoja de aceptación de firma electrónica de los servidores públicos de la Oficialía Mayor del Estado de Chiapas.
6. Integración y captura de la hoja de listado de protección civil piso 7 de los servidores públicos de la Oficialía Mayor del Estado de Chiapas.
7. Registro y control de los juicios, demandas, recursos administrativos, consultas o cualquier otro trámite en que sea parte la Oficialía Mayor, sus unidades administrativas o servidores públicos que la integran y cuya defensa o intervención sea competencia de la Unidad de Asuntos Jurídicos.
8. Integración, uso y resguardo de los datos personales de los proveedores que participan en las licitaciones restringidas.
9. Integración, uso y resguardo de los datos personales de los proveedores que participan en las licitaciones públicas.
10. Registro e Inscripción al Padrón de Proveedores del Poder Ejecutivo del Estado de Chiapas.
11. Integración y resguardo de los expedientes de adjudicaciones directas.
12. Trámite de solicitudes de acceso a la Información Pública.
13. Trámite de solicitudes de Derechos ARCO y de Portabilidad.

II. El nombre, cargo y adscripción del administrador del sistema de tratamiento.

Los responsables del tratamiento de los datos personales en la Oficialía Mayor del Estado de Chiapas, son los que se describen a continuación:

Responsable	Cargo	Órgano Administrativo	Tratamiento
Lcdo. Francisco Rafael Fuentes	Oficial Mayor	Oficina de C. Oficial Mayor	-Registro de audiencias de la oficina del C. Oficial Mayor. -Control de la agenda del C. Oficial Mayor.
Lcdo. Querubín Sandoval Fernández	Jefe de la Unidad de Apoyo Administrativo	Unidad de Apoyo Administrativo	-Integración y resguardo de los expedientes laborales de los Servidores Públicos de la Oficialía Mayor del Estado de Chiapas. -Integración y resguardo de las nóminas de pago de los servidores públicos de la Oficialía Mayor del Estado de Chiapas. -Integración y resguardo de la hoja de aceptación de firma electrónica de los servidores públicos de la Oficialía Mayor del Estado de Chiapas. -Integración y captura de la hoja de listado de protección civil piso 7 de los servidores públicos de la Oficialía Mayor del Estado de Chiapas.
Lcdo. Isidro García Alpuche	Jefe de la Unidad de Asuntos Jurídicos	Unidad de Asuntos Jurídicos	-Registro y control de los juicios, demandas, recursos administrativos, consultas o cualquier otro trámite en que sea parte la Oficialía Mayor, sus unidades administrativas o servidores públicos que la integran y cuya defensa o intervención sea competencia de la Unidad de Asuntos Jurídicos.
Lcdo. Guillermo Arena Sánchez	Director de Procesos Licitatorios	Dirección de Procesos Licitatorios	-Integración, uso y resguardo de los datos personales de proveedores que participan en las licitaciones restringidas. -Integración, uso y resguardo de los datos personales de los proveedores que participan en las licitaciones públicas. -Registro e Inscripción al Padrón de Proveedores del Poder Ejecutivo del Estado de Chiapas.
Lcda. Angélica María Vázquez Cruz	Directora de Adquisiciones de Bienes y Servicios	Dirección de Adquisiciones de Bienes y Servicios	-Integración y resguardo de los expedientes de adjudicaciones directas.
Ing. José Domingo Ocaña Clemente	Jefe del Área de Transparencia	Área de Transparencia	-Trámite de solicitudes de acceso a la Información Pública. -Trámite de solicitudes de Derechos ARCO y de Portabilidad.

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

Funciones:

- Tratar los datos personales con responsabilidad y las medidas de seguridad que se hayan establecido para tal fin.
- Resguardar los datos personales a los que tengan acceso en el ejercicio de sus atribuciones.
- Verificar que el inventario de datos personales y de los sistemas de tratamiento de los mismos, a los que tienen acceso, se encuentren actualizados.
- Llevar un registro de los servidores públicos que accedan a los datos personales y llevar a cabo las acciones necesarias para 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 en un plazo máximo de setenta y dos horas al titular, al Instituto y llevar el registro de los hechos.

Obligaciones:

- Llevar a cabo permanentemente las medidas de seguridad necesarias para la protección de los datos personales, evitando daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado, así como también garantizar la confidencialidad, integridad y disponibilidad de los mismos.
- Acatar 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.
- Guardar confidencialidad sobre la información que se conozca en el desarrollo de sus actividades.

IV. Los datos personales tratados en los sistemas de tratamientos y/o base de datos personales son los siguientes:

- Nombres y Apellidos.
- Credencial para votar.
- Clave Única de Registro de Población.
- Registro Federal de Contribuyente.
- Domicilio.
- Número de Teléfono Fijo o Celular.
- Correo Electrónico.
- Acta de Nacimiento.
- Pasaporte.
- Número de seguridad social.
- Licencia de manejo.
- Firma.

- Nivel Educativo.
- Títulos o Constancias Académicas.
- Datos Bancarios.
- Currículum Vitae.
- Estado Civil.
- Edad.
- Género.
- Certificado médico.
- Lugar y fecha de nacimiento.

Adicional a lo anterior, se recaban los siguientes datos que se consideran sensibles: Estado de salud presente (tipo de sangre, alergias, padecimientos y capacidades diferentes)

V. La descripción del sistema de tratamiento, señalando el tipo de soporte y las características del lugar donde se resguardan.

Descripción del Sistema de Tratamiento	Tipo de Soporte	Características del lugar de resguardo
1. Los datos personales son inscritos en el registro de audiencia con el C. Oficial Mayor y posteriormente pasan a integrar el archivo de trámite.	Físico	Los expedientes se encuentran resguardados en la oficina del C. Oficial Mayor, en el Piso 7, de la Torre Chiapas
2. Los datos personales son ingresados a la agenda del C. Oficial Mayor, para poder estar comunicado con los titulares de los datos y posteriormente pasar a integrar el archivo de trámite.	Físico y Electrónico	Los expedientes se encuentran resguardados en la Oficina del C. oficial Mayor, en el Piso 7, de la Torre Chiapas
3. Se elaboran los expedientes personales de cada servidor público, para el control y seguimiento de los datos personales tratados para: -Alimentar el Sistema de Nóminas del Estado de Chiapas (NECH), Plataforma (SIREH) y el Software de Control de Asistencia de Personal (DOCE). -Solicitar evaluación ante la Dirección de Evaluación y Formación de la Secretaría de Hacienda. -Afiliación al Seguro Social (IMSS). -Transferirlos a los Órganos Garantes en materia de Transparencia y a las instancias facultadas de la Administración Pública para solventar juicios legales en materia laboral y auditorias. -Guarda y custodia en los expedientes de los servidores públicos dados de baja. -La transferencia de plazas a otras dependencias. -Dar cumplimiento a las solicitudes de derechos ARCO y de portabilidad.	Físico y Electrónico	Los expedientes se encuentran resguardados en el archivero metálico con llave de seguridad al interior de la oficina que ocupa el Área de Recursos Humanos, bajo la seguridad de chapa con llave; así como en el equipo de cómputo designado al Área, en el Piso 7, de la Torre Chiapas

-Integrar el Inventario de Datos Personales.		
4. Se integran y resguardan las hojas de nómina quincenal firmadas por cada servidor público, de conformidad al pago de salario del periodo correspondiente, mismas que pueden ser transferidas a los trabajadores para trámites de pensión o por jubilación, a los Órganos Garantes en materia de transparencia y a las instancias facultadas de la administración pública para solventar juicios en materia laboral o auditorias.	Físico y Electrónico	Los expedientes se encuentran resguardados en el archivero metálico con llave de seguridad al interior de la oficina que ocupa el Área de Recursos Humanos, bajo la seguridad de chapa con llave; así como en el equipo de cómputo designado al Área, en el Piso 7, de la Torre Chiapas.
5. Se integran y resguardan las hojas de aceptación de firma electrónica por cada servidor público, mediante el cual manifiesta tener conocimiento de las obligaciones legales que conlleva el uso de dicha la firma; así mismo los datos personales son adjuntados y digitalizados en los sistemas generadores de la firma electrónica.	Físico y Electrónico	Los expedientes se encuentran resguardados en el archivero metálico con llave de seguridad al interior de la oficina que ocupa el Área de Recursos Materiales y Servicios Generales, bajo la seguridad de chapa con llave; así como en el equipo de cómputo designado al Área, en el Piso 7, de la Torre Chiapas.
6. Se integran y capturan los datos generales, así como también los padecimientos, capacidades diferentes y datos de contacto en caso de emergencia de cada servidor público de la Oficialía Mayor del Estado de Chiapas.	Físico y Electrónico	Los expedientes se encuentran resguardados en el archivero metálico con llave de seguridad al interior de la oficina que ocupa el Área de Recursos Humanos, bajo la seguridad de chapa con llave; así como en el equipo de cómputo designado al enlace de protección civil, en el Piso 7, de la Torre Chiapas.
7. Los datos personales son tratados para la integración y resguardo de los expedientes de los procesos de juicios, demandas, recursos administrativos, consultas o cualquier otro trámite en que sea parte la Oficialía Mayor, sus unidades administrativas o servidores públicos que la integran y cuya defensa o intervención sea competencia de la Unidad de Asuntos Jurídicos.	Físico	Los expedientes se encuentran resguardados en el archivero número 1, en la oficina de la Unidad de Asuntos jurídicos, en el Piso 7, de la Torre Chiapas.
8. Los datos personales son tratados para llevar a cabo los procedimientos de licitaciones restringidas, se integran desde el procedimiento de apertura técnica y económica hasta terminar el procedimiento de contratación por medio de un pedido o contrato y al final quedan en resguardo del jefe de departamento de licitaciones restringidas.	Físico y Electrónico	Los expedientes se encuentran resguardados en la oficina del Departamento de Licitaciones Restringidas, en el Piso 7, de la Torre Chiapas.
9. Los datos personales son tratados para llevar a cabo los procedimientos de licitaciones públicas, se integran desde el	Físico y Electrónico	Los expedientes se encuentran resguardados en la oficina del

procedimiento de apertura técnica y económica hasta terminar el procedimiento de contratación por medio de un pedido o contrato y al final quedan en resguardo del jefe de departamento de licitaciones públicas.		Departamento de Licitaciones Públicas, en el Piso 7, de la Torre Chiapas.
10. Los datos personales son tratados para realizar el procedimiento de Inscripción al Padrón de Proveedores del Poder Ejecutivo del Estado de Chiapas, los cuales quedan a resguardo de la jefa del Departamento de Padrón de Proveedores.	Físico y Electrónico	Los expedientes se encuentran resguardados en la oficina del Departamento de Padrón de Proveedores, en el Piso 7, de la Torre Chiapas.
11. Los datos personales son tratados para integrar un directorio interno de proveedores, llevar un control de las solicitudes de adjudicación, solicitar cotización de bienes o servicios con precios de referencia de mercado, enlistarlos en el dictamen comparativo de precios de mercado, para participar como proveedor en una adjudicación directa, para notificar en caso de ser el proveedor adjudicado, integrar los expedientes de resguardo de los procesos de adjudicación directa.	Físico	Los expedientes se localizan en cajas de archivo apilados dentro de la oficina tipo sala que se encuentra ubicada a un costado de la oficina principal de la Directora de Adquisiciones de Bienes y Servicios, en el piso 7 de la torre Chiapas.
12. Los datos personales son tratados en la elaboración y resguardo de los expedientes del trámite interno de las solicitudes de acceso a la Información Pública	Físico	Los expedientes se encuentran organizados en el archivero número 1, en el Área de Transparencia, en el Piso 7, de la Torre Chiapas.
13. Los datos personales son tratados en la Integración y custodia de los expedientes del trámite interno de las solicitudes de Derechos ARCO y de Portabilidad, que posteriormente pasaran a integrar el inventario general de datos personales.	Físico y electrónico	Los expedientes se encuentran organizados en el archivero número 1, en el Área de Transparencia, en el Piso 7, de la Torre Chiapas

VI. Los controles y mecanismos de seguridad para las transferencias que, en su caso, se efectúen.

Para implementar las medidas de seguridad aplicables a la transferencia de datos con las dependencias y entidades del Poder Ejecutivo en el ejercicio de sus atribuciones, el receptor de los datos personales asumirá el carácter de responsable conforme a la legislación en la materia y deberá tratar los datos personales atendiendo a dicha legislación y a lo convenido en el aviso de privacidad que le será comunicado por el Órgano Administrativo responsable transferente, quien deberá considerar la modalidad por la cual se envían los datos personales a los destinatarios, pudiendo hacerse mediante el traslado de soportes físicos, electrónicos o a través del correo electrónico Institucional. Cada una de estas modalidades se deberá sujetarse a lo siguiente:

a) Traslado de soportes físicos: En esta modalidad los datos personales se trasladan en medios de almacenamiento que se descifran a simple vista y que no requiere de ningún aparato que procese su

contenido para examinar, modificar o almacenar los datos. Por ejemplo, cuando una dependencia envía por correspondencia oficios o formularios impresos.

b) Traslado físico de soportes electrónicos: En esta modalidad se trasladan físicamente para entregar al destinatario los datos personales en archivos electrónicos contenidos en medios de almacenamiento que requieren el uso de algún aparato con circuitos electrónicos que procesen su contenido para examinar, modificar o almacenar los datos. Por ejemplo, cuando una institución entrega a otra por mensajería oficial un archivo electrónico con datos personales contenidos en discos flexibles, discos compactos o dispositivos de memoria USB, entre otros.

c) Traslado sobre redes electrónicas: En esta modalidad se transmiten los datos personales en archivos electrónicos mediante una red electrónica. Por ejemplo, cuando un archivo electrónico con un listado de proveedores se envía a una dependencia o entidad por Internet.

VII. El resguardo de los soportes físicos de los datos personales.

Los expedientes físicos se encuentran en resguardado y custodia de los responsables del sistema de tratamiento de los datos personales en el área asignada para tal efecto.

VIII. Las bitácoras de acceso y vulneraciones a la seguridad de los datos personales.

Los datos que se registran en la **Bitácora de acceso** (anexo 1) son los siguientes:

- Quien accede a los datos personales, cargo y adscripción;
- Fecha y hora en la que se realiza el acceso o se intenta el mismo, así como fecha y hora de salida;
- Propósito del acceso;
- Número del expediente utilizado;
- Tipo de soporte; y
- Firma de quien autoriza el acceso.

Los datos que se registran en la **Bitácora de vulneraciones** (anexo 2) son los siguientes:

- Fecha y hora de la vulneración;
- Motivo de la vulneración;
- Acciones correctivas y definitivas implementadas;
- Persona que resolvió la vulneración;
- Fecha y hora de notificación de la vulneración a los titulares de los datos personales comprometidos o afectados y al Órgano Garante en materia de protección de datos personales; y
- Los oficios, documentos, expedientes, estantes o archiveros dañados y los recuperados.

IX. El análisis de riesgos.

Los datos personales a los que los servidores públicos adscritos a la Oficialía Mayor tienen acceso en el ejercicio de sus atribuciones, se resguardan de manera física y/o electrónica, según las necesidades de la actividad para la cual se lleva a cabo su tratamiento.

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 los órganos administrativos de este Sujeto Obligado.

- No disponer de un lugar seguro y con acceso restringido en donde se puedan archivar los datos personales en físico.
- Permitir a todo servidor público o personas ajenas a la Oficialía Mayor, el acceso a los expedientes que contienen datos personales.
- Pérdida de expedientes físicos debido a catástrofes naturales, plagas o 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 los servidores públicos en relación con la confidencialidad que deben guardar sobre los datos personales que traten debido al desempeño de sus funciones.
- Pérdida, robo o extravío de expedientes.
- Alteración de la información.

Análisis de dichos riesgos, amenazas y sus posibles vulneraciones

Amenaza	**Vulnerabilidades**	**Posibles consecuencias**
Acceso de personas no autorizadas a los sistemas.	Adquirir información de los titulares de los 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 psicológica 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 otros servidores públicos, 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 y 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 y 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 personales y la pérdida, robo o extravío de expedientes.	Daño de los datos personales, pérdida de los datos personales o modificaciones no autorizadas.

X. El 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 los órganos administrativos de este Sujeto Obligado se encuentran susceptibles de enfrentar, podemos realizar el análisis de brecha de las medidas de seguridad existentes:

- El acceso se tiene restringido, una vez que el dato se encuentra en posesión de los órganos administrativos, estos se ubican fuera del alcance de los ciudadanos.
- Cada oficina cuenta con puertas que separan el área al momento de terminar labores.

- Las llaves que se tienen en las áreas se encuentran en manos de servidores públicos, autorizados por cada área.

- El servidor público genera un expediente para cada trámite de los datos personales, ya sea físico o electrónico.

- Una vez realizado el expediente o carpeta de manera física o electrónica, es guardada en archiveros o puesta en resguardo, solo tendrán acceso los servidores públicos facultados para hacerlo.

- Una vez que los datos personales se encuentren en posesión de los órganos administrativos, en caso de que se les dé proceso electrónico, el servidor público guarda los mismos en carpeta electrónica, ya sea en su computadora, carpeta compartida, correo electrónico oficial o plataforma.

- Una vez concluido el trámite de los datos personales, 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 el área.

XI. La gestión de vulneraciones.

En caso de ocurrir alguna vulneración deberá registrarse en la bitácora de contingencias, además de informar de forma inmediata al titular de los datos personales y al Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Chiapas, las vulneraciones de seguridad ocurridas, que afecten o impacten de forma significativa los derechos patrimoniales o morales del titular de los datos personales, en un plazo máximo de setenta y dos horas en cuanto se confirmen y este en proceso las acciones encaminadas para dimensionar la afectación, con la finalidad de que los titulares de los datos personales puedan tomar medidas correspondientes para la defensa de sus derechos, dicha notificación debe contener lo siguiente:

- La naturaleza del incidente.
- Los datos personales comprometidos.
- Las recomendaciones y medidas que el titular puede adoptar para proteger sus intereses.
- Las acciones correctivas realizadas de forma inmediata.
- Los medios donde puede obtener mayor información al respecto.

Al ocurrir una vulneración de seguridad, el servidor público 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.

XII. Las medidas de seguridad físicas aplicadas a las instalaciones.

Los servidores públicos adscritos a la Oficialía Mayor que traten datos personales en el ejercicio de sus funciones y/o atribuciones, observarán al menos, las medidas de seguridad siguientes:

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

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

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

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

XIII. Los controles de identificación y autenticación de usuarios.

Los titulares de los órganos administrativos de este Sujeto Obligado responsables del tratamiento y acceso a los datos personales resguardados, designarán a los servidores públicos que tendrán autorizado tratar los datos personales y acceder a los expedientes en resguardo.

XIV. Los procedimientos de respaldo y recuperación de datos personales.

En la medida de lo posible se deben almacenar los documentos físicos en medio electrónico, es decir, capturar, digitalizar o escanear la información en papel para almacenarla, de forma tal que se resguarde el mínimo de información en papel y solamente se imprima cuando sea estrictamente necesario. Esto debido a que es más práctico respaldar información copiando un archivo de un medio electrónico a otro, que fotocopiar, organizar y almacenar documentos en papel.

Los datos personales almacenados en equipo de cómputo pueden dañarse de manera parcial o total debido a fallas en los sistemas o aplicaciones, por errores de operación de las personas, o bien por interrupciones de energía eléctrica, si se realizan respaldos de la información importante de manera periódica pueden mitigarse las consecuencias de estos incidentes. Es fundamental que los respaldos se efectúen de manera regular y también cada vez que haya una actualización importante de los datos que están siendo almacenados en la organización. Se pueden realizar respaldos parciales únicamente de la información crítica, diario o cada semana, y respaldos de toda la información, cada quince días o mensualmente. Es importante que los respaldos no se encuentren en la misma ubicación física que la información que se están respaldando y hacer pruebas de recuperación de las copias de respaldo para asegurarnos de que la información se encuentra íntegra.

XV. El plan de contingencia.

Las acciones deben atenderse considerando:

- El análisis y revisión de la falla o incidente;

- Determinar las causas que dieron origen a la falla o incidente;
- Evaluar las acciones necesarias para evitar que la falla o incidente vuelva a ocurrir;
- Determinar e implementar las acciones necesarias;
- Registrar los resultados de las acciones tomadas; y
- Revisar la eficacia de las acciones correctivas tomadas.

XVI. Las técnicas utilizadas para la supresión y borrado seguro de los datos personales.

Si cualquier documento es depositado simplemente en la basura, éste puede ser recuperado y visto por cualquier persona malintencionada, y así ocurrir una fuga de información importante. Por otra parte, en los medios electrónicos, la simple acción de "borrado" no elimina de forma definitiva la información, y ésta puede ser recuperada desde los dispositivos desechados, con ciertas herramientas.

Por ello se deben tomar en cuenta controles como:

- *Destrucción segura de documentos:* Los documentos y otros medios físicos no deben simplemente desecharse una vez que ya no se utilizan, sino destruirse por ejemplo con triturador o incinerado. Cuando se adquiere equipo para estas tareas se debe evaluar que tan difícil sería para una persona recuperar la información, por ejemplo, hay trituradoras que hacen tiras el papel y otras que lo hacen pequeños trozos. Con tiempo y esfuerzo es posible recuperar un documento hecho tiras, pero es muy difícil recuperar uno hecho "confeti" o cenizas. Otra opción es almacenar en un sitio seguro los documentos a triturar y entregarlos periódicamente a alguien que preste el servicio de destrucción de documentos, sin olvidar que debe existir un contrato que estipule claramente el deber de confidencialidad del prestador de servicio.

- *Destrucción segura de información en equipo de cómputo y medios de almacenamiento electrónico:* Es conocido que en los equipos de cómputo se puede "borrar" o "eliminar" la información de forma simple o con un clic, pero debido a la naturaleza del almacenamiento electrónico, lo que ocurre en realidad, es que ésta deja de ser fácilmente accesible, pero sigue ahí hasta que nueva información la "sobrescribe". Para la eliminación definitiva de información existen herramientas de software que borran archivos electrónicos específicos o dispositivos de almacenamiento completos. Cuando la vida útil de un equipo de cómputo o medio de almacenamiento electrónico ha terminado, es recomendable destruirlo físicamente. Esto lo puede hacer la misma organización o contratar a un tercero para este servicio, cuando la cantidad de equipo de cómputo es mayor.

- *Fijar periodos de retención y destrucción de información:* Es importante identificar de manera regular toda la información que ya no es de utilidad para la organización y que no requiere almacenarse para cumplir con alguna responsabilidad legal o contractual. Los procedimientos de eliminación de información de gran valor o a gran escala deben ser formales y se deben registrarse en bitácoras.

- *Tomar precauciones con los procedimientos de reutilización:* Por diversas razones las organizaciones pueden optar por diferentes mecanismos de reciclado para minimizar costos, pero se debe ser cuidadoso en la posible exposición de datos personales. Por ejemplo, es común

el uso de "bandejas de papel reciclado", pero bajo ninguna circunstancia deberían utilizarse documentos con datos personales como "papel de reúso". Cuando el equipo de cómputo tenga que cambiar de dueño por ejemplo, de un empleado a otro, es importante respaldar la información relevante para la organización y borrar completamente los datos que resguarda el equipo.

XVII. El plan de trabajo.

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 Documento de Seguridad de los Datos Personales.

Por ello, se deben establecer y mantener programas de capacitación para:

a) La difusión en general de la protección de datos personales en la organización;

b) Instruir al personal de manera específica respecto a sus funciones y responsabilidad en el tratamiento y seguridad de los datos personales; y

c) Incluir la seguridad en el tratamiento de los datos personales dentro de la cultura de los servidores públicos.

XVIII. Los mecanismos de monitoreo y revisión de las medidas de seguridad.

Se debe monitorear y revisar el riesgo con sus factores relacionados, es decir, 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.

XIX. El programa general de capacitación.

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, en ese sentido, se plantea generar un programa para desarrollar la cultura en materia de seguridad y protección de datos personales, conforme a lo siguiente:

a) *Sensibilización* en materia de Protección de Datos Personales en la Oficialía Mayor y su importancia en el entorno laboral.

b) Capacitación a las y los servidores públicos, enlaces en materia de Datos Personales respecto los mecanismos, medios y procedimientos disponibles para ejercer los *Derechos ARCOP*.

c) Concientizar a las y los servidores públicos que dentro de sus funciones y obligaciones se encuentren la de recabar los datos personales, respecto a la importancia de informar al titular de los datos personales a través del *aviso de privacidad,* el tratamiento de los mismos.

d) Capacitar a las y los servidores públicos que cuentan con la facultad de autorizar, acordar y/o decidir en el Órgano Administrativo, respecto a la implementación de las *Medidas de Seguridad Administrativa, Técnicas y Físicas* para la Protección de los Datos Personales.

e) Asesorar a las y los servidores públicos que dentro de sus atribuciones se encuentre el tratamiento de los datos personales, respecto a la implementación del *Documento de Seguridad*.

Anexo 1

Bitácora de acceso a los Datos Personales en los archivos de (trámite o concentración) **físicos o base de Datos Personales del ejercicio** (año en curso).

Órgano Administrativo (o en su caso Área generadora o resguardante): _____
Responsable del Archivo (trámite o concentración): _____

Hoja 1 de 1

No. Cons.	Nombres y apellidos	Cargo y adscripción	Fecha y hora de acceso	Fecha y Hora de salida	Propósito del acceso	Número del expediente utilizado	Tipo de soporte	Firma de autorización
1								
2								
3								
4								

Anexo 2

Bitácora de vulneraciones a la seguridad de los Datos Personales en los archivos de (trámite o concentración) **físicos o base de Datos Personales del ejercicio** (año en curso).

Órgano Administrativo (o en su caso Área generadora o resguardante): _____
Responsable del Archivo (trámite o concentración): _____

Hoja 1 de 1

No. Cons.	Fecha y hora de la vulneración	Motivo de la vulneración	Acciones correctivas implementadas y el responsable de implantarlas	Acciones definitivas implementadas y el responsable de implantarlas	Fecha y hora de notificación de la vulneración a los titulares de los datos personales afectados	Fecha y hora de notificación al Órgano Garante en materia de protección de datos personales	Los datos personales comprometidos o dañados	Los datos personales y/o expedientes recuperados
1								
2								
3								
4								

Lcdo. Querubín Sandoval Fernández.
Titular de la Unidad de Apoyo Administrativo y Presidente del Comité de Transparencia.

Lcdo. Isidro García Alpuche.
Titular de la Unidad de Asuntos Jurídicos y Secretario Técnico del Comité de Transparencia.

Lcda. Angélica María Vázquez Cruz
Titular de la Dirección de Adquisiciones de Bienes y Servicios, Titular del Área Coordinadora de Archivo y Vocal del Comité de Transparencia.

HOJA PROTOCOLARIA DE FIRMAS DE APROBACIÓN Y AUTORIZACIÓN DEL DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE LOS DATOS PERSONALES EN POSESIÓN DE LA OFICIALÍA MAYOR DEL ESTADO DE CHIAPAS, DEL ACTA DE LA DÉCIMA OCTAVA SESIÓN DEL COMITÉ DE TRANSPARENCIA, DE FECHA 07 DE SEPTIEMBRE DE 2022.