De la mano con el Pueblo
VILLA COMALTITLÁN
GOBIERNO MUNICIPAL 2024-2027

HUMANISMO QUE TRANSFORMA

DOCUMENTO DE SEGURIDAD

H. AYUNTAMIENTO DE VILLA COMALTITLÁN, CHIAPAS.

UNIDAD DE TRANSPARENCIA

PROTECCIÓN DE DATOS PERSONALES

PALACIO MUNICIPAL S/N, COLONIA CENTRO, PLANTA ALTA
VILLA COMALTITLAN, CHIAPAS.
TELEFONOS: 9641391382
E-MAIL: Secretariamunicipalvilla.24.27@gmail.com

ÍNDICE

1. INTRODUCCIÓN..... 3

2. -OBJETIVOS Y ALCANCES DEL DOCUMENTO. 4

2.1.- Objetivos generales.....4

2.2.- Objetivos específicos.....4

2.3.- Alcance del documento. 5

3.- SISTEMA DE GESTIÓN DE SEGURIDAD DE LOS DATOS PERSONALES EN POSESIÓN DEL H. AYUNTAMIENTO DE VILLA COMALTITLÁN CHIAPAS..... 6

4.- INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO. 13

CATEGORÍAS DE DATOS PERSONALES 13

5. - FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATAN DATOS PERSONALES..... 17

6. - ANALISÍS DE RIESGO Y BRECHA 19

7. - GESTIÓN DE VULNERACIONES Y PLAN DE CONTINGENCIA..... 27

8. - MEDIDAS DE SEGURIDAD GENERALES 29

A. Medidas administrativas.....29

B. Medidas físicas 30

C. Medidas técnicas.....30

MONITOREO DE LAS MEDIDAS DE DEGURIDAD.....31

9. - PLAN DE TRABAJO PARA LA IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD 33

10. - PROPUESTA DE CAPACITACIÓN EN MATERIA DE DATOS PERSONALES..... 35

11. - ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD..... 36

12. - VIGENCIA, APROBACIÓN Y OBSERVANCIA DEL DOCUMENTO DE SEGURIDAD 37

1. INTRODUCCIÓN

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.

En este sentido la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas (LPDPPSOCHIS) establece un conjunto de bases principios y procedimientos para garantizar el derecho a la protección de datos con carácter personal y que se encuentren en posesión de los sujetos obligados, entre los que figura el H. Ayuntamiento de Villa Comaltitlán, Chiapas.

De ahí que 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 del H. Ayuntamiento de Villa Comaltitlán; Chiapas, por las diversas unidades administrativas que conforman su estructura orgánica, 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.

En ese sentido, el H. Ayuntamiento de Villa Comaltitlán; Chiapas, ha identificado los procesos que se llevan a cabo en el ámbito de su competencia, en los que se utilizan datos personales, a efecto de mantener la seguridad de los mismos durante el ciclo de vida de la información, indicando la forma en la que se trata, las medidas de seguridad adoptadas y las áreas responsables de su protección, así como las finalidades del tratamiento de acuerdo a sus respectivas funciones que desempeñan.

Considerando que los datos personales constituyen el principal activo de información objeto del presente documento, Lo que se busca es crear un sistema de gestión para el tratamiento de los datos personales 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 del H. Ayuntamiento de Villa Comaltitlán, Chiapas, se entiende por sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, operar, monitorear, mantener y mejorar el tratamiento y seguridad de los datos personales.

Esto implica el planteamiento de acciones conducentes para evitar la alteración, pérdida, transmisión y acceso no autorizado de los datos mediante la implementación de medidas físicas, administrativas y técnicas, tendientes a garantizar la seguridad e integridad de los mismos, así como su seguimiento y supervisión continua. De ahí, que dicho Sistema permita disponer de información relacionada con las medidas de seguridad, el análisis general de las amenazas y posibles vulnerabilidades, así como los mecanismos o acciones a implementar para mitigarlas. Incluye además acciones que permitan controlar y verificar que el tratamiento de los datos personales se realice de acuerdo con los principios establecidos para la protección de los datos personales, implicando un compromiso con las disposiciones previstas en la ley y en los lineamientos generales, por parte de los funcionarios involucrados.

Finalmente, ante la necesidad de mantener actualizado el documento de seguridad se ha de procurar la mejora continua, además, se ha procedido a la actualización de los elementos que integran el documento de seguridad; las medidas de seguridad adoptadas en su tratamiento, el análisis de riesgo y brecha, que permiten dar seguimiento a las medidas adoptadas, identificar las posibles vulneraciones y aminorar los riesgos. Todo lo anterior, acompañado del desarrollo del programa de capacitación que permita comprender la importancia de adoptar medidas para la prevención de las vulneraciones a los datos personales.

2.- OBJETIVOS Y ALCANCES DEL DOCUMENTO.

2.1.- Objetivos generales.

El presente documento tiene como objetivo:

Establecer los principales elementos que integran las medidas de seguridad administrativas, físicas y técnicas necesarias para la protección de los datos personales en posesión del H. Ayuntamiento de Villa Comaltitlán; Chiapas, como un medio para cumplir con las obligaciones que establece la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de Chiapas y los Lineamientos Generales, para garantizar la confidencialidad, integridad y disponibilidad de los datos personales; así como determinar las posibles vulnerabilidades, amenazas y riesgos de los que pueden ser objeto. así como la normatividad que derive de los mismos; estableciendo con ello, los elementos y actividades de gestión para la operación y control de los procesos que impliquen el tratamiento de datos personales, a efecto de protegerlos de manera sistemática y continua, y promover la adopción de mejores prácticas en relación con la protección de datos personales. para establecer las bases, criterios y mecanismos necesarios para garantizar la adecuada protección de los datos personales que se encuentran bajo posesión y responsabilidad del H. Ayuntamiento Municipal de Villa Comaltitlán, Chiapas, en cumplimiento de las obligaciones previstas en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas (LPDPPSOCHIS), los Lineamientos Generales y demás disposiciones normativas aplicables.

2.2.- Objetivos específicos.

• Identificar áreas responsables: Localizar las unidades administrativas que manejan datos personales.

• Asignar roles: Definir quiénes son los responsables y usuarios autorizados de la información.

• Establecer controles: Fijar las medidas de seguridad y los mecanismos de monitoreo para su aplicación correcta.

• Gestionar riesgos: Detectar riesgos y brechas de seguridad para tomar decisiones de mejora continua.

• Capacitar al personal: Fomentar una cultura de buenas prácticas y conciencia sobre el manejo de la información.

2.3.- Alcance del documento.

El alcance de este presente documento de seguridad se relaciona con la identificación de sistemas de información o procesos administrados por parte de todas las unidades administrativas que realicen tratamientos de datos personales en ejercicio de sus atribuciones, y a todos los tratamientos de datos personales que efectúen, mismos que se encuentran bajo su estricta responsabilidad, tanto en los medios electrónicos como en los espacios físicos en que se administran, operan y administran, con observancia de los principios, deberes y obligaciones que establece la ley.

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

Las unidades administrativas que forman parte del H. Ayuntamiento de Villa Comaltitlán, Chiapas y que deberán observar el Programa de Protección de Datos Personales son las siguientes:

Presidencia Municipal
Sindicatura Municipal
Órgano Interno de Control
Secretaria Municipal
Tesorería Municipal
Dirección de obras Publicas
Oficialía Mayor
Fomento Agropecuario
Unidad de transparencia
Jurídico
Protección Civil
Secretario Ejecutivo de Seguridad Publica
Seguridad Pública Municipal
Juzgado Municipal
Defensoría de los Derechos Humanos
DIF Municipal
SAPAM

Asimismo, cualquier otra unidad administrativa que forme parte de la estructura del Ayuntamiento y que realice actividades de tratamiento de datos personales deberá cumplir con las disposiciones establecidas en este instrumento de seguridad. La Unidad de Transparencia integra este documento de seguridad con base en la información generada por todas las unidades administrativas que conforman el H. Ayuntamiento de Villa Comaltitlán, Chiapas.

3.- SISTEMA DE GESTIÓN DE SEGURIDAD DE LOS DATOS PERSONALES EN POSESIÓN DEL H. AYUNTAMIENTO DE VILLA COMALTITLÁN CHIAPAS.

De conformidad con los artículos 77 y 78 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, el Comité de Transparencia del H. Ayuntamiento Municipal de Villa Comaltitlán, Chiapas, es la máxima autoridad interna en materia de protección de datos personales y tendrá a su cargo coordinar y supervisar las acciones necesarias para garantizar su adecuada protección en el tratamiento de los datos personales que lleva a cabo el H. Ayuntamiento de Villa Comaltitlán; Chiapas, garantiza el tratamiento de los datos personales que lleva a cabo como parte de sus funcione desde 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 de estos datos, 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.

Por lo anterior el H. Ayuntamiento de Villa Comaltitlán inició un proceso de organización y planeación de los medios para la 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 la institución, se involucra el tratamiento de datos personales. Para ello, se dispuso de un formato que facilitó a las diversas unidades administrativas, realizar el levantamiento de inventarios de los datos personales que se encuentran bajo su responsabilidad, considerando lo establecido en el artículo 47 de la Ley de Protección de Datos Personales del Estado de Chiapas; logrando con ello 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 para la consideración del ciclo de vida de los datos personales, entendiendo 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, lo que cobra especial relevancia en el marco del proceso de baja documental que las áreas realizan conforme a las disposiciones que regulan la gestión documental al interior del Ayuntamiento de Villa Comaltitlán.

De igual forma, Una vez integrados los inventarios de tratamientos y de datos, se dispuso de la metodología para el análisis de riesgos, con la intención de que se identificaran el valor de los datos de acuerdo a su categoría y su ciclo de vida, así como el valor de exposición, las posibles consecuencias para los titulares por el uso indebido y/o posible vulneración y las condiciones de riesgo a los que podrían encontrarse expuestos por medidas de seguridad poco confiables. Lo anterior, permitió identificar la brecha entre las medidas de seguridad existentes y las medidas de seguridad faltantes para que garanticen la seguridad de los datos, tanto administrativas, como físicas y técnicas.

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, tal y como se ilustra a continuación el siguiente esquema

Considerando que la identificación de posibles vulneraciones tiene por objeto prevenir posibles debilidades en la seguridad de los datos y las áreas de oportunidad, aun cuando no haya existido un daño real, mediante la identificación de la ineficiencia de los controles de acceso físico y electrónicos

y el inadecuado establecimiento de los esquemas de privilegios, sumado al poco conocimiento de procesos y responsabilidades en materia de protección de datos personales, además de la falta de definición de perfiles y roles, falta de seguimiento y monitoreo a los medios de seguridad y la inexistencia de mecanismos para garantizar la confidencialidad por parte del personal.

algunos tipos de amenazas, que pueden ser intencionales o no, a las que podría enfrentarse la institución y sus activos de información.

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

El riesgo que de manera general puede presentarse en caso de que las amenazas señaladas exploten las vulnerabilidades, es el de facilitar el acceso a los datos personales de manera no autorizada comprometiendo su confidencialidad, disponibilidad e integridad; por lo que las medidas de seguridad por parte de las áreas comisionadas están orientadas a proteger los datos personales. A partir de la identificación de vulnerabilidades y amenazas, se han establecido medidas de seguridad generales, que de acuerdo a la experiencia y mejores prácticas son monitoreadas para lograr la mejora continua por parte de todos los involucrados en el tratamiento. En el marco del sistema de gestión y política de seguridad institucional, se procurará:

- Tratar datos personales de manera lícita, conforme a las disposiciones establecidas.
- Informar a los titulares del tratamiento de los datos y sus finalidades;
- Sujetar el tratamiento de datos personales al principio de consentimiento salvo las excepcionas previstas por la Ley;
- Procurar que los datos personales tratados sean correctos y estén actualizados;
- Suprimir los datos personales cuando hayan dejado de ser necesarios para las
- finalidades para las cuales se obtuvieron;
- Tratar los datos personales estrictamente para propósitos legales o legítimos para el cual fueron obtenidos y estrictamente los necesarios para las finalidades;
- No obtener datos personales a través de medios fraudulentos;
- Velar por el cumplimiento de los principios, estableciendo y manteniendo medidas de seguridad y de confidencialidad durante el ciclo de vida de los datos personales, en estricto respeto de los derechos de los titulares;

- Mantener actualizado el inventario de datos personales que maneja el H. Ayuntamiento de Villa Comaltitlán;
- Respetar los derechos de los titulares en relación con sus datos personales;
- Identificar a los servidores públicos del Ayuntamiento de Villa Comaltitlán responsables del tratamiento de los datos personales;

Con base en lo anterior, el Ayuntamiento de Villa Comaltitlán determina las pautas de acción del personal encargado de tratamiento de datos personales con intención a generar su correcto resguardo, buscando en todo momento actuar en apego a las disposiciones de la LGPDPPSO y los Lineamientos de la materia, siempre en consideración de la protección del derecho a la privacidad y protección de datos de las personas.
Con base en lo anterior, y tomando como punto de partida la identificación de vulnerabilidades y amenazas, se han establecido medidas de seguridad generales, que, de acuerdo con otras experiencia y mejores prácticas tomadas como referencia, se encaminan a la mejora continua por parte de las personas involucradas en el tratamiento, en la búsqueda de logar la salvaguarda del derecho a la privacidad y protección de datos personales, se han determinado las líneas de acción para el personal encargado de tratamiento de datos, con el propósito de generar mecanismos para el resguardo adecuado, actuando en apego a la LPDPPSO de Chiapas y los lineamientos correspondientes.

De acuerdo con el artículo 29 de la Ley, deberán identificarse las funciones y obligaciones del personal que participe en el tratamiento de datos personales, por lo que cada área deberá establecer las responsabilidades que correspondan a sus servidores públicos.

El H. Ayuntamiento Municipal de Villa Comaltitlán, Chiapas, establecerá y mantendrá mecanismos para garantizar la adecuada protección de los datos personales que se encuentren bajo su responsabilidad, desde su obtención hasta su eliminación, conservación o cualquier otra forma de tratamiento, procurando en todo momento preservar su confidencialidad, integridad y disponibilidad. Para ello, las unidades administrativas identificarán los procesos y actividades en los que se realice tratamiento de datos personales, considerando las funciones que les corresponden y las finalidades para las cuales la información es obtenida.

Como parte del sistema de gestión, se realizarán análisis de riesgos y de brecha, con la finalidad de identificar las amenazas y vulnerabilidades que puedan afectar los datos personales, así como determinar las medidas de seguridad necesarias para disminuir los riesgos identificados.

Las medidas de seguridad podrán ser de carácter administrativo, físico y técnico, y estarán orientadas a prevenir situaciones como el robo, extravío, pérdida, alteración, destrucción, acceso, uso o tratamiento no autorizado de los datos personales.

Las unidades administrativas deberán mantener controles adecuados para proteger la información y procurar la mejora continua de las medidas implementadas. Asimismo, deberán promover entre el personal una cultura de protección de datos personales y establecer claramente las funciones y responsabilidades de quienes intervengan en su tratamiento.

En el marco de este sistema de gestión, el Ayuntamiento procurará:

- Tratar los datos personales de manera lícita y conforme a las disposiciones aplicables.
- Utilizar los datos únicamente para las finalidades que justificaron su obtención.
- Procurar que los datos personales sean adecuados, correctos y, cuando corresponda, actualizados.
- Mantener la confidencialidad y seguridad de la información durante su ciclo de vida.
- Respetar los derechos de las personas titulares de los datos personales.
- Identificar al personal autorizado para intervenir en el tratamiento de los datos.
- Implementar medidas administrativas, físicas y técnicas para prevenir vulneraciones.
- Capacitar y sensibilizar al personal respecto de sus obligaciones en materia de protección de datos personales.

Con estas acciones, el H. Ayuntamiento Municipal de Villa Comaltitlán, Chiapas, fortalecerá la gestión y protección de los datos personales bajo su responsabilidad, mediante la identificación de riesgos, la implementación de medidas de seguridad y la revisión periódica de los controles establecidos.

ESQUEMA

la identificación de vulnerabilidades tiene por objeto prevenir posibles dificultades en la seguridad de los datos bajo un enfoque proactivo; es decir, identificar áreas de oportunidad en materia de seguridad de datos personales sin que éstas constituyan un daño efectivo, es que se listan como posibles vulnerabilidades, las siguientes:

1. Falta de controles para acceder a los sistemas de tratamiento de datos personales.

2. Negligencia en el tratamiento de datos.
3. Reproducción no autorizada de los datos
4. Destrucción total o parcial no autorizada.
5. Divulgación no autorizada de los datos.

La determinación del nivel de riesgo deberá considerar tanto la probabilidad de que ocurra una vulneración como el impacto que esta pudiera generar en las personas titulares.

Entre las principales amenazas que deberán considerarse dentro del análisis se encuentran:

- Robo, extravío o copia no autorizada de los datos personales.
- Acceso, uso o tratamiento no autorizado.
- Daño, alteración o modificación no autorizada de la información.
- Pérdida o destrucción de los datos personales.

A partir de los resultados obtenidos, el H. Ayuntamiento Municipal de Villa Comaltitlán, Chiapas, podrá determinar las medidas de seguridad que deberán implementarse o fortalecerse en cada unidad administrativa, así como las acciones necesarias para atender las deficiencias identificadas mediante el análisis de brecha.

Los resultados de ambos análisis deberán servir como base para la elaboración y seguimiento del plan de trabajo correspondiente, procurando que las medidas de seguridad sean revisadas y mejoradas de manera periódica. De esta forma, el Ayuntamiento podrá fortalecer progresivamente la protección de los datos personales y mantener condiciones adecuadas de confidencialidad, integridad y disponibilidad de la información bajo su responsabilidad.

4.- INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO.

Para cumplir con los objetivos y obligaciones es necesario que cada una de las unidades administrativas identifiquen los procesos en los que actualmente se lleva a cabo tratamiento de datos personales; obteniendo con ello el denominado Inventario de Datos Personales.

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

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

- Presidencia Municipal
- Sindicatura Municipal
- Órgano Interno de Control
- Jurídico
- Secretaria Municipal
- Tesorería Municipal
- Dirección de obras Publicas
- Fomento Agropecuario
- Unidad de transparencia
- Oficialía Mayor
- Protección Civil

- Secretario Ejecutivo de Seguridad Publica
- Seguridad Pública Municipal
- Juzgado Municipal
- Defensoría de los Derechos Humanos
- DIF Municipal
- SAPAM

Todos los tratamientos se realizan en apego a sus facultades y obligaciones que la normatividad les confiere, a través de las diversas áreas que lo integran y permiten el desarrollo de los procesos que realizan para el cumplimiento de dichas funciones.

En base a lo anterior, fue posible identificar 80 procesos que se desarrollan, que implican el tratamiento de datos personales. que a continuación se describen:

Tratamiento de Datos Personales por Unidad Administrativa

A continuación, se describen las unidades administrativas, áreas correspondientes y los procesos o tratamientos de datos personales que llevan a cabo:

Unidad Administrativa	Área o Departamento	Proceso o Tratamiento
Presidencia Municipal	Presidencia Municipal	Atención a la Ciudadanía
Sindicatura Municipal	Sindicatura Municipal	Juicios Civiles Juicios Laborales Juicios Administrativos Procedimientos y Juicios Penales
Jurídico	Jurídico	Juicios Civiles Juicios Laborales Juicios Administrativos Procedimientos y Juicios Penales
Órgano Interno de Control	Órgano Interno de Control	Tramitación de Medios de Impugnación (Recursos de Revisión y Denuncias por incumplimiento por obligaciones de transparencia) Elaboración de Contratos Expediente único de personal Proceso de entrega-Recepción Declaración de situación patrimonial
		Convenios Elaboración de Constancias (identidad, concubinato, ingreso económico, en la elaboración de la constancia de bilingüismo)
Secretaría Municipal	Secretaría Municipal	Elaboración de Constancias (bajos recursos económicos, dependencia económica, constancia de origen) Registro de Fierro Marcador Validación de Cartillas Elaboración de Nombramientos Actas de Cabildo Invitaciones Certificación Trámite de Cartilla de Servicio Militar Trámites para Demolición de Templos y Construcción
Tesorería Municipal	Tesorería Municipal	Nómina de Personal Expediente Único de Personal Comprobación para diferentes tipos de gastos Padrón de Proveedores

		Cobro de Ingresos
Dirección de Obras Públicas	Dirección de Obras Públicas	Padrón de Contratistas Elaboración de Contratos Expediente de Obras Registro de Contratistas Padrón de Beneficiarios Comprobaciones Supervisiones de Obras
Fomento Agropecuario	Fomento Agropecuario	Padrón de Beneficiarios Comprobaciones
Unidad de Transparencia	Unidad de Transparencia	Atención a las Solicitudes de Acceso a la Información y de Datos Personales Seguimiento al Directorio de los Sujetos Obligados Integración y actualización de la Unidad de Transparencia Actualización de las Obligaciones de Transparencia Seguimiento de denuncias por incumplimiento de las Obligaciones de Transparencia Integración del Comité de Transparencia
Protección Civil	Protección Civil	Lista de Asistencia Expediente del Personal Expediente Único de Personal
Consejo Municipal de Seguridad Pública	Consejo Municipal de Seguridad Pública	Convenios y Contratos Trámite de carta laboral Certificado del Centro Estatal de Control y Confianza
Seguridad Pública Municipal	Seguridad Pública Municipal	Registro de Detenidos Notificaciones Requisitos para cumplir con los lineamientos (Nacionalidad) Apoyo de Traslados (enfermos, ataúd, auxilios) Alta de Elementos en el sistema Seguro Social o Seguro de Vida
Juzgado Municipal	Juzgado Municipal	Juicios Civiles Asuntos Familiares (Separación, régimen de visitas, guarda y custodia) Asuntos Mercantiles (elaboración de Pagarés)
Juez Calificador	Juez Calificador	Actos Conciliatorios Sanciones Administrativas Canalización a Rehabilitación
Defensoría de los Derechos Humanos	Defensoría de los Derechos Humanos	Denuncia en la Fiscalía del Ministerio Público Acuerdo en Reparación de Daños Atención en la Fiscalía Envió de notificaciones Incumplimiento de asistencia familiar o violencia familiar
DIF Municipal	Presidencia y Dirección	Traslados Apoyo económico Nómina de Personal Pago de Proveedores Expediente Único de Personal
DIF Municipal	Desayunos Escolares	Salud Alimentaria (Maternidad Segura, Menores de 5 Años, Desayunos Escolares) Proyecto SAS
DIF Municipal	Procuraduría	Violencia Familiar

		Guarda y Custodia
DIF Municipal	Psicología	Para estadísticas Control de asistencia
DIF Municipal	UBR (Unidad Básica de Rehabilitación)	Para estadísticas Para brindar el servicio Control de asistencia
DIF Municipal	Casa de Día	Control de asistencia
DIF Municipal	Trabajo Social	Estudio socioeconómico

CATEGORIAS DE DATOS PEROSNALES
luego de un proceso de análisis, como resultado se identificaron también los datos personales que se utilizan en los tratamientos, que corresponden a las tres categorías, tal como se señala a continuación:

De identificación

Firma, Nombre de la Persona Física, Antecedentes Laborales, CURP, RFC, Estado Civil, Cedula Profesional, Año de nacimiento o Edad, Beneficiarios, Correo electrónico Personal, Curriculum Vitae, Datos Académicos, Datos contenidos en declaraciones patrimoniales, Datos de identificación, Datos de Salud, Domicilio, Huella Dactilar, Menor de Edad, Nacionalidad, Nivel Educativo, Ocupación, Sexo, Teléfono fijo o Celular, Títulos Profesionales

Patrimoniales

Número de Cuenta, Cuentas bancarias, estados de cuenta, CLABE interbancaria, institución bancaria, facturas, Descuentos personales (ahorro voluntario, hipoteca, seguro médico, seguro de automóvil

Sensibles

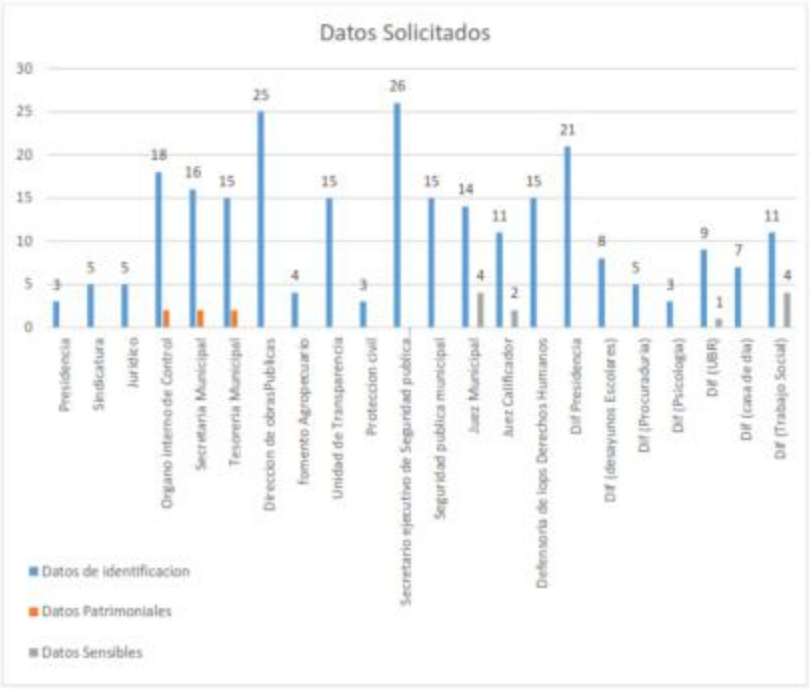
Circunstancias socioeconómicas, Creencias Religiosas, filosóficas o morales, Discapacidad, Lengua Indígena y Pertenencia a Pueblo Indígena

Estos datos son utilizados en 80 procesos, de los cuales dos corresponden a presidencia, tres a sindicatura, cuatro a la Dirección Jurídica, 3 al Órgano Interno de Control, diez a Secretaria Municipal, cinco a Tesorería Municipal, siete a la Dirección de Obras Públicas Municipales, dos de Fomento Agropecuario, 6 de Unidad de Transparencia, dos de Protección Civil, cuatro de Secretario Ejecutivo de Seguridad Pública, seis de Seguridad Pública, tres de Juzgado Municipal, tres de Juzgado Calificador, cinco de Defensoría de Derechos Humanos, siete DIF presidencia, dos DIF Desayunos Escolares, 2 DIF Psicología, 3 DIF UBR, uno DIF Casa de Día, uno DIF trabajo. Asimismo, en 75 procesos se utilizan datos personales de identificación, en 3 se utilizan datos personales patrimoniales y en cuatro procesos se utilizan datos sensibles.

Anexar grafica proceso por unidad administrativa

Como se puede observar en la gráfica, el área que desarrollan mayor número de procesos es el área de secretaria Municipal, mientras que el DIF Municipal en el área de casa de día y Trabajo Social son las que menos procesos realizan, al ser solamente uno en cada área.

De todos los datos solicitados, todas las áreas solicitan datos de identificación, mientras que solamente el Área de Órgano Interno de Control, secretaria Municipal y Tesorería Municipal solicitan datos patrimoniales y el Área de Juzgado municipal, Juzgado calificador y Trabajo Social del DIF Municipal solicitan datos sensibles; tal como se observa en la siguiente gráfica.



en relación con los procesos en los que se tratan datos personales, el 100 por ciento de los procesos usa datos identificativos, el 13.6 por ciento usa datos patrimoniales, y el 18.18 por ciento usa datos sensibles, como se muestra a continuación:

Como resultado, podemos identificar que la categoría de datos personales con mayor número de áreas y procesos es de carácter identificativo, el segundo los que incluyen datos sensibles y como terceros datos patrimoniales que se utilizan en cuatro procesos. Asimismo, hay que señalar que se identificaron cuatro procesos que realizan tratamiento de datos tanto identificativos como patrimoniales.

Datos solicitados

Es posible observar que Secretaria Municipal, la Dirección de Obras Públicas y el DIF Municipal son las áreas que desarrollan el mayor número de procesos en los que se tratan datos personales, de acuerdo a sus atribuciones y obligaciones, lo anterior, debido a que las áreas que la integran se encuentran aquellas que cuentan con atribuciones para administrar los recursos humanos, materiales y financieros del ayuntamiento; lo cual implica que los procesos correspondientes a la protección de datos personales sean aplicados con mayor cuidado y puntualidad. por lo tanto, esas áreas que cuentan con mayor número de procesos, en materia de protección de datos deben contar con un enfoque de importancia en el desarrollo de las actividades.

Se logró identificar que las áreas tienen un medio diferente a las demás para obtener los datos personales, y estos son: físicamente, correo electrónico y redes sociales; siempre directamente con el titular. No existe un sistema de base de datos del Ayuntamiento donde se puedan guardar los datos personales; si no que cada área se encarga de buscar y desarrollar estrategias para brindarle mayor protección a los datos personales, mediante archiveros o software para poder almacenar de manera electrónica en los equipos de cómputo.

El inventario de datos personales del Ayuntamiento de Villa Comaltitlán, se integra como un elemento del sistema de gestión de datos personales, en base a los hallazgos identificados en su actualización que junto con las medidas de seguridad representa un instrumento útil para la implementación de las medidas necesarias en materia de protección de datos personales.

Así mismo, ayuda a planear capacitaciones enfocados en materia protección de datos hacia los funcionarios del H. Ayuntamiento de Villa Comaltitlán, teniendo como objetivo preparar y sensibilizar a los funcionarios para los tratamientos que ellos realizan de conformidad con los estándares nacionales e internacionales en la materia. En tal virtud se consolida el inventario de datos personales del H. Ayuntamiento de Villa Comaltitlán, Chiapas, como un elemento de la política implementada para la observancia de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados aportando con ello certeza a la ciudadanía sobre cual es y cuales son el destino de los datos que se recaban por este Sujeto obligado.

5.- FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATAN DATOS PERSONALES.

A consecuencia de la identificación de los procesos en los que se tratan datos personales, relacionado en el Inventario de Datos Personales, por las áreas que integran el H. Ayuntamiento de Villa Comaltitlán, Chiapas, es de suma importancia definir estas actividades con las facultades y obligaciones establecidas en la Ley de Protección de Datos Personales en posesión de Sujetos Obligados del Estado de Chiapas, que otorga a los servidores públicos responsabilidad en todo tratamiento que realicen; lo anterior, a fin de dar cumplimiento al principio de legalidad que debe atender todo servidor público. Por lo anterior, a continuación, se ilustran las atribuciones y funciones otorgadas por la Ley de Desarrollo Constitucional en Materia de Gobierno y Administración Municipal del Estado de Chiapas a quienes llevan a cabo tratamiento de datos personales.

Tabla de Funciones y Servidores Públicos

Área Administrativa	Cargo de la(s) persona(s) funcionaria(s) que trata(n) datos personales	Funciones	Acciones
Presidencia Municipal	Dr. Gerardo Pérez Gómez	Ejecutar las decisiones del Ayuntamiento, ser el conducto para presentar las iniciativas de Ley en materia municipal, cumplir y hacer cumplir las leyes y reglamentos aplicables en el Municipio.	Atender las necesidades primordiales que las autoridades solicitan para el bienestar de la localidad y la del municipio.
Sindicatura Municipal	Lic. Ana Isanel Arrieta Chiñas	Vigilar y defender los intereses municipales, vigilar la correcta aplicación de los recursos financieros conforme al presupuesto aprobado, representar jurídicamente al Ayuntamiento, procurar la justicia y legalidad en la administración pública municipal.	Representación legal del Ayuntamiento, con carácter de mandatario judicial, así como el trámite y la resolución de los asuntos que sean de su competencia.
Jurídico	Lic. Víctor Manuel Infante Toledo	Realizar los estudios e investigaciones jurídicas que requiera el desarrollo del Municipio; defender los intereses del municipio en todo tipo de procedimientos judiciales.	Coordinar los programas de normatividad del municipio.
Órgano Interno de Control	C.P. José Alonso Alturzar Pérez	Vigilar el ejercicio del gasto público y su congruencia con el presupuesto de egresos del Municipio.	Juzga las cuentas de las personas o funcionarios que tienen a su cargo fondos o bienes públicos, con el objeto de hacer efectiva su responsabilidad patrimonial.
Secretaría Municipal	Lic. Guadalupe Esperanza Pimentel Cardona	Atender asuntos de carácter administrativo y para... Auxiliar en sus funciones al presidente Municipal.	Planear, coordinar, ejecutar planes, programas, proyectos y acciones que... Permitan dar seguimiento y satisfacer las diversas demandas ciudadanas. Atender y resolver los asuntos administrativos que le encomiende el ayuntamiento.
Tesorería Municipal	Fernando Guzman Simón	Organizar y llevar la contabilidad del municipio y los registros necesarios para el control de las partidas presupuestales para el registro contable de las operaciones y transacciones que se lleven a cabo, las cuentas de activo, pasivo, patrimonio, ingresos, costos y gastos se manejarán conforme a las normas y procedimientos que dicte la Ley de Presupuesto, Contabilidad y Gasto Público Municipal y el Órgano de Fiscalización Superior del Congreso del Estado.	Rinda cuentas claras a la ciudadanía y facilite el pago oportuno a los contribuyentes mediante la automatización de procesos, logrando incrementar la recaudación de ingresos.

Área Administrativa	Cargo de la(s) persona(s) funcionaria(s) que trata(n) datos personales	Funciones	Acciones
Dirección de Obras Públicas	Ing. José Armando Espinoza Medina	Regular, proyectar, construir, presupuestar, contratar, adjudicar, conservar y ejecutar las obras públicas del Municipio, cuando así corresponda conforme al marco legal aplicable y a las normas dictadas al respecto por el Gobernador del Estado.	Planear, administrar, organizar, dirigir, supervisar y evaluar obras y acciones que permitan el desarrollo en infraestructura y equipamiento urbano y rural en el municipio, para brindar un servicio de eficiencia y calidad a la ciudadanía.
Fomento Agropecuario	Ing. Williams Pérez Roblero	Impulsar el desarrollo en el sector agropecuario, de servicios y comercio mediante la capacitación y la gestión de proyectos productivos ante instituciones federales, estatales y demás fuentes financieras con el fin de mejorar las condiciones socioeconómicas de los productores y de sus familias.	Proporcionar los recursos humanos y materiales que le permitan atender, promover, gestionar, vincular, generar, coordinar y operar con eficiencia, todos los programas y proyectos derivados del Proyecto Municipal.
Unidad de Transparencia	Ing. Francisco Spond Gonzalez	Atender Solicitudes de Acceso a la Información Pública y de Datos Personales.	Atender Solicitudes de Acceso a la Información Pública y de Datos Personales.
Protección Civil	Javier Antonio Verdugo Fernández	Priorizar la prevención de riesgos, prestar auxilio, priorizar el análisis y gestión prospectiva de riesgos de desastres.	Prevención, reducción y mitigación de riesgos. Preparación y alerta. Respuesta a la emergencia.
Secretario Ejecutivo de Seguridad Pública	Lic. Deysy Alas Amaya	Formular lineamientos para el establecimiento de políticas municipales en materia de seguridad pública.	Proponer a los presidentes municipales reformas a reglamentos municipales en materia de Seguridad Pública;
Seguridad Pública Municipal	Lic. Luis Alberto de la Paz Quintana	Velar, coordinar y controlar acciones para hacer respetar las disposiciones contenidas en el Bando de Policía y Gobierno y demás disposiciones legales en materia de seguridad pública aplicables en el Municipio.	Coadyuvar en las labores de protección civil o auxilio de la población cuando se requiera.
Juzgado Municipal	Lic. Luis Fernando López Vázquez	Administrar Justicia en el Municipio, dotada de jurisdicción para decidir litigios.	Conocer, calificar e imponer las sanciones administrativas municipales que procedan por faltas o infracciones a los ordenamientos municipales.
Juez	Lic. Luis Fernando López Vázquez	Encargado de resolver las controversias y sancionar las faltas o infracciones administrativas, cometidas en el territorio del municipio.	Imponer una multa, o bien, retenerle en arresto preventivo de acuerdo a la ley.
Defensoría de los Derechos Humanos	Lic. Julio Ozuna Santos	Se constituye como el enlace de coordinación entre las organizaciones no gubernamentales y la Comisión de Derechos Humanos del Estado de México, sin perjuicio de las demás atribuciones que establece la Ley de la Comisión de Derechos Humanos del Estado de México.	Asesorar y orientar a los habitantes de su municipio, en especial a los menores, mujeres, adultos mayores, personas en discapacidad, indígenas y detenidos o arrestados, a fin de que les sean respetados sus derechos humanos.
DIF Municipal	Lic. Laura Laguna Morales	Fortalecer y satisfacer las necesidades de asistencia social y prestación de servicios asistenciales, proporcionando soluciones eficientes de gran impacto que beneficien a la población más vulnerable y contribuyan al mejor desarrollo de las familias.	Jornadas Integrales. Asesoría Jurídica. Atención médica. Campañas Preventivas (suicidios/adicciones/cáncer, etc). Transporte Adaptado. Eventos Especiales. Programas de Asistencia.

6.- ANALISÍS DE RIESGO Y BRECHA

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD, APARTADO DEL ANÁLISIS DE RIESGO Y BRECHA.

Se testa el apartado número 6, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II,

112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD, APARTADO DEL ANÁLISIS DE RIESGO Y BRECHA.

Se testa el apartado número 6, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II,

112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD, APARTADO DEL ANÁLISIS DE RIESGO Y BRECHA.

Se testa el apartado número 6, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II,

112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD, APARTADO DEL ANÁLISIS DE RIESGO Y BRECHA.

Se testa el apartado número 6, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II,

112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD, APARTADO DEL ANÁLISIS DE RIESGO Y BRECHA.

Se testa el apartado número 6, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II,

112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD, APARTADO DEL ANÁLISIS DE RIESGO Y BRECHA.

Se testa el apartado número 6, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II,

112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD, APARTADO DEL ANÁLISIS DE RIESGO Y BRECHA.

Se testa el apartado número 6, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II,

112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD, APARTADO DEL ANÁLISIS DE RIESGO Y BRECHA.

Se testa el apartado número 6, que contiene el Análisis de Riesgo y Brecha, contiene información que identifica las vulnerabilidades, debilidades, amenazas y deficiencias de las medidas de seguridad implementadas por el sujeto obligado. Su divulgación podría facilitar accesos no autorizados, vulneraciones de datos personales o afectar la eficacia de los controles de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II,

112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

7. - GESTIÓN DE VULNERACIONES Y PLAN DE CONTINGENCIA.

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD, APARTADO DEL GESTIÓN DE VULNERACIONES Y PLAN DE CONTINGENCIA

Se testa el apartado número 7, que contiene la Gestión de Vulneraciones y Plan de contingencia, toda vez que contiene información sensible sobre la forma en que el sujeto obligado previene, detecta, contiene, responde y recupera la operación ante incidentes de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

SECCIÓN CLASIFICADA DEL DOCUMENTO DE SEGURIDAD, APARTADO DEL GESTIÓN DE VULNERACIONES Y PLAN DE CONTINGENCIA

Se testa el apartado número 7, que contiene la Gestión de Vulneraciones y Plan de contingencia, toda vez que contiene información sensible sobre la forma en que el sujeto obligado previene, detecta, contiene, responde y recupera la operación ante incidentes de seguridad, de conformidad con lo dispuesto en los artículos 103, fracción II, 112 fracción VI, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo vigésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

8 - MEDIDAS DE SEGURIDAD GENERALES

Conforme al análisis de brecha, existen algunas medidas de seguridad que se requiere implementar, por lo que a continuación se presentan las actividades generales que se planea realizar las medidas de seguridad administrativas, físicas y técnicas tienen como finalidad proteger los datos personales que son tratados por el H. Ayuntamiento Municipal de Villa Comaltitlán, Chiapas, y reducir los riesgos que puedan afectar su confidencialidad, integridad y disponibilidad. Estas medidas deberán aplicarse de acuerdo con las características de cada tratamiento, los medios utilizados para el manejo de la información y el nivel de riesgo identificado. Su implementación estará orientada a prevenir situaciones como pérdida, extravío, daño, destrucción, alteración, acceso, uso, tratamiento o divulgación no autorizada de los datos personales.

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

Para fortalecer la protección de la información, se consideran las siguientes medidas:

A. Medidas administrativas
I. Capacitación y sensibilización.

Promover actividades de capacitación dirigidas a las personas servidoras públicas que intervienen en el tratamiento de datos personales, con el propósito de fortalecer sus conocimientos sobre los principios, deberes, obligaciones y medidas de seguridad establecidos en la legislación vigente.

II. Control de documentos y expedientes.
Establecer mecanismos para controlar la recepción, préstamo, consulta y devolución de documentos y expedientes que contengan datos personales, procurando mantener un registro que permita identificar su ubicación y las personas que hayan tenido acceso a ellos.

III. Resguardo de la información.
Implementar procedimientos para el adecuado manejo y resguardo de expedientes y documentos que contengan datos personales, considerando las disposiciones aplicables en materia de gestión documental y archivos.

IV. Compromiso de confidencialidad.
Establecer mecanismos mediante los cuales las personas servidoras públicas que tengan acceso a datos personales conozcan y asuman el deber de confidencialidad respecto de la información que manejen con motivo de sus funciones.

V. Registro y atención de incidencias.
Establecer mecanismos para reportar, registrar y dar seguimiento a incidentes relacionados con la seguridad de los datos personales, con la finalidad de identificar sus causas y adoptar las acciones preventivas o correctivas correspondientes.

B. Medidas físicas

I. Protección de documentos físicos.

Resguardar los expedientes, documentos y demás soportes físicos que contengan datos personales en espacios destinados para su conservación, procurando que permanezcan protegidos contra pérdida, daño, deterioro, sustracción o acceso de personas no autorizadas.

II. Control de acceso a las instalaciones.

Establecer mecanismos de control para limitar el acceso a las áreas en las que se encuentren documentos, archivos, equipos o cualquier otro medio que contenga datos personales, permitiendo el ingreso únicamente a las personas autorizadas.

III. Protección de equipos y espacios de trabajo.

Procurar que los equipos de cómputo, escritorios, archiveros, cajones y demás espacios utilizados para el tratamiento de datos personales permanezcan bajo condiciones que reduzcan el riesgo de acceso o consulta por personas no autorizadas.

IV. Protección frente a factores ambientales.

Adoptar medidas razonables para prevenir daños ocasionados por factores como humedad, polvo, incendios, filtraciones de agua u otras circunstancias que puedan afectar los documentos y soportes que contengan datos personales.

C. Medidas técnicas

I. Control de usuarios y contraseñas.

Utilizar cuentas de usuario y contraseñas individuales para el acceso a los equipos y sistemas que contengan datos personales, evitando compartirlas, prestarlas o dejarlas expuestas. Las contraseñas deberán contar con características que dificulten su identificación o descifrado por personas no autorizadas.

II. Protección de credenciales de acceso.

Cuando se detecte que una cuenta, usuario o contraseña pudo haber sido utilizada por una persona no autorizada, deberá informarse oportunamente al responsable correspondiente para adoptar las medidas necesarias, incluyendo el cambio o bloqueo de las credenciales comprometidas.

III. Uso de medios institucionales.

Procurar que las actividades laborales que involucren datos personales se realicen mediante cuentas de correo electrónico, sistemas y herramientas institucionales

autorizadas, evitando utilizar medios personales o no autorizados para almacenar o transmitir información.

IV. Protección de archivos electrónicos.

Mantener los documentos y archivos electrónicos que contengan datos personales bajo mecanismos de protección adecuados, tales como contraseñas, permisos de acceso u otros controles disponibles, de acuerdo con las características de los equipos y sistemas utilizados.

V. Control de impresión y reproducción.

Evitar que documentos impresos que contengan datos personales permanezcan expuestos o sean abandonados en impresoras, copiadoras, escritorios u otros espacios de uso común. Las copias y reproducciones deberán realizarse únicamente cuando sean necesarias para el cumplimiento de las funciones correspondientes.

VI. Respaldo de información.
Cuando la naturaleza del tratamiento lo requiera, establecer mecanismos de respaldo de la información electrónica para reducir el riesgo de pérdida o destrucción de los datos personales y facilitar su recuperación ante incidentes.

VII. Actualización y protección de equipos.
Mantener los equipos y sistemas utilizados para el tratamiento de datos personales en condiciones adecuadas de funcionamiento y, cuando corresponda, aplicar actualizaciones y mecanismos de protección que contribuyan a reducir vulnerabilidades de seguridad.

Las medidas señaladas deberán ser observadas por las unidades administrativas y por las personas servidoras públicas que intervengan en el tratamiento de datos personales. Su aplicación deberá revisarse periódicamente y fortalecerse de acuerdo con los resultados del análisis de riesgos y de brecha, así como con las modificaciones que se presenten en los procesos, sistemas o medios utilizados por el Ayuntamiento. La implementación progresiva de estas medidas permitirá al H. Ayuntamiento Municipal de Villa Comaltitlán, Chiapas, fortalecer las condiciones de seguridad de los datos personales bajo su responsabilidad y reducir la posibilidad de que se presenten vulneraciones que puedan afectar los derechos y libertades de las personas titulares.

MONITOREO DE LAS MEDIDAS DE SEGURIDAD
El monitoreo de las medidas de seguridad constituye una actividad necesaria para verificar que los controles administrativos, físicos y técnicos implementados para la protección de los datos personales sean adecuados y se mantengan en condiciones de funcionamiento. Esta supervisión permitirá detectar oportunamente posibles deficiencias, vulnerabilidades o situaciones que puedan poner en riesgo la información bajo responsabilidad del H. Ayuntamiento Municipal de Villa Comaltitlán, Chiapas.

La revisión de las medidas de seguridad deberá realizarse de manera periódica y considerar las características de los procesos, los medios utilizados para el tratamiento de los datos personales y los riesgos identificados. Los resultados obtenidos podrán utilizarse para establecer acciones preventivas, correctivas y de mejora continua.

Entre las acciones de monitoreo que podrán realizarse se consideran las siguientes:

1. Revisión de contraseñas y mecanismos de acceso.
Verificar periódicamente que las contraseñas y demás mecanismos utilizados para acceder a equipos o sistemas que contengan datos personales sean individuales, seguras y se encuentren bajo control de las personas autorizadas, evitando su divulgación o uso compartido.

2. Supervisión de las medidas de seguridad.
Revisar periódicamente el cumplimiento de las medidas administrativas, físicas y técnicas establecidas para la protección de los datos personales, identificando aquellas que requieran actualización, fortalecimiento o corrección.

3. Control de acceso a las áreas de resguardo.
Verificar que el ingreso a los espacios donde se encuentren documentos, expedientes, equipos o sistemas que contengan datos personales se encuentre limitado al personal autorizado y que, cuando corresponda, existan mecanismos para identificar y controlar el acceso de personas externas.

4. Revisión de equipos y espacios de trabajo.
Supervisar que los equipos de cómputo, archivos, escritorios, impresoras y demás espacios utilizados para el tratamiento de datos personales mantengan condiciones adecuadas de seguridad y que la información no permanezca expuesta innecesariamente.

5. Seguimiento de incidencias.
Dar seguimiento a los reportes relacionados con posibles vulneraciones o incidentes de seguridad, procurando identificar sus causas, consecuencias y medidas necesarias para evitar que vuelvan a presentarse.

6. Evaluación y mejora continua.
Utilizar los resultados obtenidos mediante el monitoreo para fortalecer las medidas de seguridad y, cuando sea necesario, establecer nuevas acciones de protección de acuerdo con los cambios en los procesos, sistemas, tecnologías o niveles de riesgo.

El monitoreo deberá realizarse de manera coordinada entre las unidades administrativas responsables de los tratamientos y las áreas que, de acuerdo con sus atribuciones, participen en la protección de la información. Las observaciones y resultados derivados de estas actividades deberán considerarse para mantener actualizadas las medidas de seguridad y contribuir a la mejora continua del sistema de gestión de datos personales del H. Ayuntamiento Municipal de Villa Comaltitlán,
Chiapas.

9.- PLAN DE TRABAJO PARA LA IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD

Sección Clasificada del Documento de Seguridad, apartado del Plan de Trabajo.

Se testa el apartado número 9, que contiene el Plan de Trabajo, en virtud de ser un instrumento de gestión que deriva del análisis de riesgo y del análisis de brecha, en él se establecen las acciones específicas que el sujeto obligado implementará para corregir deficiencias, fortalecer controles y reducir los riesgos identificados, cuya divulgación podría comprometer la seguridad del sistema de tratamiento de datos personales, de conformidad con lo dispuesto en los artículos 103, fracción III, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo trigésimo octavo de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas

Sección Clasificada del Documento de Seguridad, apartado del Plan de Trabajo.

Se testa el apartado número 9, que contiene el Plan de Trabajo, en virtud de ser un instrumento de gestión que deriva del análisis de riesgo y del análisis de brecha, en él se establecen las acciones específicas que el sujeto obligado implementará para corregir deficiencias, fortalecer controles y reducir los riesgos identificados, cuya divulgación podría comprometer la seguridad del sistema de tratamiento de datos personales, de conformidad con lo dispuesto en los artículos 103, fracción III, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas y en los artículos 3, fracción IX, y 6, párrafo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, así como en el artículo trigésimo octavo de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas

10. - PROPUESTA DE CAPACITACIÓN EN MATERIA DE DATOS PERSONALES

La aplicación del programa de protección de datos personales en el ayuntamiento de Villa Comaltitlán, requiere como un factor esencial, la formación y sensibilización de las personas que ahí laboran, de tal forma que pueda garantizarse la actualización y mejora continua del inventario de datos personales, la observancia de la normatividad y Ley, por lo que se propone un programa de capacitación en el tema de protección de datos personales que favorezca la profundización en el conocimiento del tema por parte de quienes intervienen en el tratamiento de datos personales. A manera de propuesta, se han considerado los siguientes temas:

La Ley de protección de datos personales en posesión de sujetos obligados en Chiapas.

- Antecedentes
- Principios.
- Alcances
- Objetivo
- Implicaciones

II) Obligaciones en la observancia de la LPDPPSOCHIS

- Deberes.
- Medidas de seguridad.
- Procedimientos y sanciones/ Derechos ARCO (acceso,

rectificación, cancelación y oposición).

- Medios de defensa.

III) El programa de protección de datos personales

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

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

- Contenido: Integral, simplificado
- Consentimiento.
- Deber de información.
- Finalidades del tratamiento de los datos

11. - ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD.

El H. Ayuntamiento Municipal de Villa Comaltitlán, Chiapas, deberá mantener actualizado este Documento de Seguridad, de conformidad con lo establecido en el artículo 30 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, con la finalidad de que las medidas de protección correspondan a las condiciones reales en que se lleva a cabo el tratamiento de los datos personales.

La actualización deberá realizarse cuando se produzcan modificaciones sustanciales en los tratamientos de datos personales que impliquen un cambio en el nivel de riesgo, así como cuando, derivado del monitoreo, revisión y mejora continua del sistema de gestión, se identifiquen aspectos que requieran ser modificados o fortalecidos. También deberá actualizarse cuando sea necesario establecer acciones para mitigar los efectos de una vulneración de seguridad o cuando, como consecuencia de ésta, se determinen medidas correctivas y preventivas que deban incorporarse al sistema de protección de datos personales.

Las modificaciones que se realicen deberán considerar, según corresponda, los resultados del análisis de riesgos y de brecha, las medidas de seguridad administrativas, físicas y técnicas, las funciones y responsabilidades de las áreas involucradas y las acciones previstas en el plan de trabajo.

Con independencia de los supuestos anteriores, el Documento de Seguridad será revisado por lo menos una vez al año, con el propósito de verificar que su contenido se encuentre actualizado y sea acorde con los procesos, tratamientos, sistemas, medios y condiciones de seguridad existentes en el H. Ayuntamiento.

De cada revisión o actualización deberá procurarse dejar constancia de los cambios realizados, las causas que los originaron y, cuando corresponda, las acciones que deberán implementarse para fortalecer la protección de los datos personales.

Cuando de la revisión resulte necesario modificar el Documento de Seguridad, éste deberá someterse nuevamente a consideración y, en su caso, aprobación del Comité de Transparencia del H. Ayuntamiento Municipal de Villa Comaltitlán, Chiapas, atendiendo a las atribuciones que le corresponden en materia de protección de datos personales.

La actualización permanente de este instrumento permitirá al Ayuntamiento mantener un proceso de mejora continua y fortalecer las condiciones de confidencialidad, integridad y disponibilidad de los datos personales bajo su responsabilidad.

12.- VIGENCIA, APROBACIÓN Y OBSERVANCIA DEL DOCUMENTO DE SEGURIDAD

El presente Documento de Seguridad entrará en vigor a partir de la fecha en que sea aprobado por el Comité de Transparencia del H. Ayuntamiento Municipal de Villa Comaltitlán, Chiapas, y será de observancia obligatoria para las unidades administrativas y personas servidoras públicas que, con motivo de sus funciones, intervengan en el tratamiento de datos personales.

Las disposiciones contenidas en este instrumento deberán ser consideradas en las actividades relacionadas con la obtención, uso, almacenamiento, consulta, conservación, transmisión, eliminación y demás formas de tratamiento de datos personales que se realicen dentro del Ayuntamiento.

Las unidades administrativas deberán observar las medidas y responsabilidades establecidas en este Documento, así como informar oportunamente cualquier situación que pueda representar un riesgo para la seguridad de los datos personales o que requiera la modificación de las medidas implementadas.

Este Documento permanecerá vigente mientras no sea sustituido o modificado por una nueva versión aprobada por la autoridad competente. Su contenido deberá revisarse periódicamente y actualizarse cuando las condiciones de los tratamientos, los riesgos identificados, las medidas de seguridad o la legislación aplicable así lo requieran.

La aprobación, modificación y actualización del Documento de Seguridad deberá quedar debidamente documentada, señalando la fecha correspondiente y, cuando resulte aplicable, el número de sesión o acta mediante la cual haya sido aprobada.

Con la observancia de este instrumento, el H. Ayuntamiento Municipal de Villa Comaltitlán, Chiapas, reafirma su compromiso de proteger los datos personales bajo su responsabilidad y de fortalecer de manera permanente las medidas

destinadas a garantizar su confidencialidad, integridad y disponibilidad.

DOCUMENTO DE SEGURIDAD

SISTEMA DE DATOS PERSONALES DE TRANSPARENCIA PARA EL PUEBLO DE CHIAPAS

ELABORÓ:
ING. FRANCISCO SPOND GONZÁLEZ
RESPONSABLE DE LA UNIDAD DE TRANSPARENCIA

APROBÓ:
DR. GERARDO PÉRÉZ GÓMEZ
PRESIDENTE MUNICIPAL CONSTITUCIONAL DE VILLA COMALTITLÁN

FECHA DE ELABORACION DEL DOCUMENTO DE SEGURIDAD: 27 DE AGOSTO DE 2026
FECHA DE ACTUAIZACION DEL DOCUMENTO DE SEGURIDAD: 29 DE SEPTIEMBRE DE 2026