



DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES
EN POSESIÓN DEL H. AYUNTAMIENTO DE TOTOLAPA, CHIAPAS





ÍNDICE

1. PRESENTACIÓN

2. OBJETIVOS DEL DOCUMENTO DE SEGURIDAD

3. RESPONSABILIDADES

4. ALCANCE DEL DOCUMENTO DE SEGURIDAD PRINCIPIOS

4.1 LICITUD

4.2 LEALTAD

4.3 INFORMACIÓN

4.4 CONSENTIMIENTO

4.5 FINALIDAD

4.6 PROPORCIONALIDAD

4.7 CALIDAD

4.8 RESPONSABILIDAD

DEBERES

4.9 SEGURIDAD

4.10 CONFIDENCIALIDAD

5. SISTEMA DE GESTIÓN DE LOS DATOS PERSONALES

6. INVENTARIO DE TRATAMIENTOS Y DATOS PERSONALES

7. FUNCIONES Y RESPONSABILIDADES DEL TRATAMIENTO DE DATOS PERSONALES

8. PROGRAMA DE TRABAJO PARA LA IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD

9. ANÁLISIS DE RIESGO Y BRECHA

10. ANÁLISIS DE LA INFORMACIÓN

11. MEDIDAS DE SEGURIDAD

12. MONITOREO DE MEDIDAS DE SEGURIDAD

13. PROPUESTA DE CAPACITACIÓN EN MATERIA DE DATOS PERSONALES



1.- PRESENTACIÓN

En la elaboración del Documento de Seguridad se deberán tener presentes los mecanismos y los instrumentos que dan cuenta de las medidas de seguridad técnica, física y administrativa en el tratamiento de los datos personales que se adoptan en el **H. Ayuntamiento de Totolapa, Chiapas**, en sus diferentes áreas administrativas, garantizando de esta manera el cumplimiento de los procedimientos, bases y principios a la protección de datos personales establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas y lo establecido en el artículo 6º, apartado “A”, de la Constitución Política de los Estados Unidos Mexicanos, mandata el derecho que tiene toda persona respecto a la protección de sus datos personales las cuales serán protegidos en los términos y con las excepciones que fijan las leyes. Así también, toda persona tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación, cancelación y oposición (ARCO) de éstos.

Dicho lo anterior, el Derecho a la Protección de Datos Personales, tiene por objeto proveer lo necesario para garantizar plenamente el derecho que tiene toda persona a la protección de sus datos personales en posesión del **H. Ayuntamiento de Totolapa, Chiapas**, por lo que será de observancia obligatoria para todos los servidores públicos que intervienen en el tratamiento de datos personales, estableciendo planteamientos y acciones conducentes para evitar la alteración, pérdida, transmisión y acceso no autorizado de los datos, así como, acciones que permitan controlar y verificar que el tratamiento de los datos personales se realice de acuerdo a los principios establecidos mediante la implementación de medidas que garanticen la seguridad integral de los mismos, y un seguimiento y supervisión continuo de conformidad con lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.

2.- OBJETIVOS DEL DOCUMENTO DE SEGURIDAD

Ofrece los mecanismos y los instrumentos que dan cuenta de las medidas de seguridad técnica, físicas y administrativas en el tratamiento de los datos personales que se adoptan en el **H. Ayuntamiento de Totolapa, Chiapas**, garantizando de esta manera el cumplimiento de los procedimientos, bases, principios, la confidencialidad, integridad y disponibilidad a la protección de datos personales establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas y los Lineamientos Generales, así como la normatividad que derive de los mismos; estableciendo con ello, los elementos y actividades de gestión para la operación y control de los procesos que impliquen el tratamiento de datos personales, a efecto de protegerlos



de manera sistemática y continua, y promover la adopción de mejores prácticas en relación con la protección de datos personales.

3.- RESPONSABILIDADES

La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, establece en los artículos 77 y 78, en la que refiere que el Comité de Transparencia, es la autoridad máxima en materia de protección de datos personales y tiene entre sus funciones el coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, dicho órgano tendrá las siguientes funciones con relación a este programa:

- I. Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los Datos Personales en la organización del responsable, de conformidad con lo previsto en la presente Ley y demás disposiciones aplicables en la materia;
- II. Instituir, en su caso, procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes para el ejercicio de los Derechos ARCO;
- III. Confirmar, modificar o revocar las determinaciones en las que se declare la inexistencia de los Datos Personales o se niegue por cualquier causa el ejercicio de alguno de los Derechos ARCO;
- IV. Establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor observancia de la presente Ley y demás disposiciones aplicables en la materia;
- V. Supervisar, en coordinación con las áreas u órganos administrativos competentes, el cumplimiento de las medidas, controles y acciones previstas en el Documento de Seguridad;
- VI. Dar seguimiento y cumplimiento a las resoluciones emitidas por el Órgano Desconcentrado de la Secretaría o la Autoridad Garante competente, según corresponda;
- VII. Establecer programas de capacitación y actualización para las personas servidoras públicas en materia de protección de Datos Personales, y
- VIII. Dar vista al órgano de control interno u homólogo o equivalente en aquellos casos en que tenga conocimiento, en el ejercicio de sus atribuciones, de una presunta



irregularidad respecto de determinado tratamiento de Datos Personales; particularmente en casos relacionados con la declaración de inexistencia que realice el responsable”.

Las áreas administrativas y la de Transparencia tendrán las funciones y responsabilidades que se describen más adelante en este documento.

Los objetivos planteados deberán lograrse con éxito, por lo que el Programa requiere del trabajo de todos en conjunto. En ese sentido, el Programa se deberá hacer del conocimiento del Titular de la Presidencia, a fin de que tome las medidas necesarias para que el mismo se observe en el **H. Ayuntamiento de Totolapa, Chiapas**.

La Presidencia Municipal, tendrá la finalidad de impulsar la debida implementación del Programa al interior de este Sujeto Obligado, pero no podrá suplir ni afectar las funciones que otorgan los artículos 77 y 78 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas al Comité de Transparencia, en su carácter de máxima autoridad de datos personales en la Institución.

En la implementación del Programa, el resultado será el cumplimiento integral de las obligaciones que establece la LPDPPSOCHIS y los Lineamientos correspondientes, el Programa será de observancia obligatoria para todos los servidores públicos de este sujeto obligado que en el ejercicio de sus funciones traten datos personales.

Todos los servidores públicos del **H. Ayuntamiento de Totolapa, Chiapas**, que tengan acceso a los datos personales, deberán estar capacitados en materia de tratamiento de datos personales, conocer y aplicar adecuadamente las medidas de seguridad implementadas en cada sistema de tratamiento de datos personales, desde su obtención hasta su debida eliminación. Por lo que, deberán ejecutar dicho tratamiento de manera responsable y atendiendo en todo momento las medidas de seguridad propias de los sistemas; por lo que, en caso de alguna situación diversa, que genere daño, pérdida, alteración, destrucción, o su uso, acceso o tratamiento no autorizado de los datos personales, deberán comunicarlo para garantizar su confiabilidad, integridad y disponibilidad.

4.- ALCANCE DEL DOCUMENTO DE SEGURIDAD

El documento de seguridad se relaciona con la identificación de sistemas de información o procesos administrados por parte de todas las áreas administrativas que realicen tratamientos de datos personales en ejercicio de sus atribuciones, y a todos los tratamientos de datos personales que efectúen en ejercicio de sus atribuciones, mismos que se encuentran bajo su estricta responsabilidad, tanto en los medios electrónicos



H. AYUNTAMIENTO MUNICIPAL CONSTITUCIONAL DE TOTOLAPA
2024-2027
UNIDAD DE TRANSPARENCIA



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 56 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas.

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

- ✓ Secretario Municipal
- ✓ Juez Municipal
- ✓ Contralor Municipal
- ✓ Director de Obras Publicas
- ✓ Unidad de Transparencia
- ✓ DIF Municipal

El área de Transparencia integra este documento de seguridad con base en la información generada por todas las unidades administrativas que conforman el **H. Ayuntamiento de Totolapa, Chiapas.**

Es de precisar que el **H. Ayuntamiento de Totolapa, Chiapas**, es el responsable sobre el tratamiento de los datos personales que se obtengan o utilicen con motivo de las facultades establecidas en su Ley Local, y en ese sentido, todo el personal que por razón de sus funciones tenga acceso a los mismos debe atender al cumplimiento de los principios y deberes establecidos en la LPDPPSOCHIS, mismos que consisten en los siguiente:

El derecho a la protección de los datos personales se sistematiza a través de ocho principios y dos deberes:



PRINCIPIOS

Licitud
Lealtad Información
Consentimiento
Finalidad
Proporcionalidad
Calidad
Responsabilidad

DEBERES

Seguridad
Confidencialidad

Compromiso y Honestidad
que dan confianza

PRINCIPIO DE LICITUD.

Se encuentra previsto en el artículo 12 de la LPDPPSOCHIS y exige a los responsables que el tratamiento de los datos personales lo realicen observando lo que ordena la Ley. De esta forma se busca que el tratamiento de datos personales no se efectúe de manera arbitraria sino de forma objetiva.

PRINCIPIO DE LEALTAD.

El artículo 13 de la LPDPPSOCHIS ordena que el responsable no deberá obtener y tratar datos personales, a través de medios engañosos o fraudulentos, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad.

La Ley prohíbe al responsable recurrir a mecanismos ilegales o poco transparentes para recolectar y tratar los datos, los cuales deben utilizarse en la forma como se ha pactado o establecido.

PRINCIPIO DE INFORMACIÓN.

Se estipula que el titular tenga conocimiento de los principales aspectos que regirán el tratamiento de sus datos personales. En este sentido, el artículo 20 de la LPDPPSOCHIS ordena al responsable informar al titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto. Traducido en el aviso de privacidad que constituye el mecanismo idóneo para informar al titular los aspectos indicados.



PRINCIPIO DE CONSENTIMIENTO.

Asimismo, el artículo 3 de la LPDPPSOCHIS define el consentimiento como la manifestación de la voluntad libre, específica e informada del titular de los datos mediante el cual autoriza el tratamiento de sus datos personales.

Y también los artículos 14 y 15 de la LPDPPSOCHIS se precisa que el consentimiento será libre cuando no medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular; específico, cuando las finalidades sean concretas, lícita, explícitas y legítimas que justifiquen el tratamiento; e informado, cuando el titular tenga conocimiento del aviso de privacidad previo el tratamiento a que serán sometidos sus datos personales.

Adicionalmente la LPDPPSOCHIS establece que el consentimiento puede ser expreso o tácito, indicando que es tácito cuando habiéndose puesto a disposición del titular el aviso de privacidad, éste no manifieste su voluntad en sentido contrario.

PRINCIPIO DE FINALIDAD.

Este principio está consagrado en el artículo 12 de la LPDPPSOCHIS y busca que el tratamiento tenga como objetivo la realización de finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones expresas que la normatividad aplicable le confiera.

Así que, quien trate datos no puede usarlos para cualquier propósito sino para aquellos establecidos en el aviso de privacidad, salvo que cuenten con atribuciones conferidas en la ley y medie el consentimiento del titular, situación en la cual excepcionalmente podrá tratar los datos para otras finalidades.

Finalmente, este principio busca evitar que se recolecten datos para hacer con ellos lo que sea y delimita los usos que pueda darle el responsable.

PRINCIPIO DE PROPORCIONALIDAD.

En concordancia con anterior, el artículo 19 de la misma Ley, ordena que sólo se pueden tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para las finalidades concretas, explícitas lícitas y legítimas que justifiquen su tratamiento. En otras palabras, el tratamiento de datos personales sólo deberá circunscribirse a los que resulten adecuados, relevantes y no excesivos en relación con la finalidad del tratamiento.



Por lo tanto, no está permitido recolectar o usar datos que no guarden estrecha relación con la finalidad del tratamiento.

PRINCIPIO DE CALIDAD.

El artículo 17 de la Ley de la materia exige mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos y según se requiera para el cumplimiento de las finalidades concretas, explícitas lícitas y legítimas que motivaron su tratamiento.

Ahora bien, este principio también se relaciona con la vigencia de los datos, pues existe la obligación de dejar de tratar información que ya no es necesaria para cumplir con las finalidades previstas en el aviso de privacidad.

Se prevé también en este artículo, la exigencia que los datos deberán ser suprimidos, previo bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos. En ese sentido, la parte final del artículo 18 de la LPDPPSOCHIS señala que los plazos de conservación de los datos personales no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron su tratamiento, y deberán atender a las disposiciones aplicables en la materia de que se trate y considerar los valores administrativos, contables, fiscales, jurídicos e históricos de los datos personales.

En suma, los datos personales no se deben tratar indefinidamente sino sólo por el período de tiempo necesario para cumplir la finalidad para la cual fueron recolectados.

PRINCIPIO DE RESPONSABILIDAD.

Los artículos 24-26 de la LPDPPSOCHIS ordenan que se adopten medidas que garanticen que los principios de la ley y sus demás disposiciones se cumplan en la práctica.

Se exige a los responsables y encargados del tratamiento de datos personales, el adoptar medidas apropiadas para cumplir sus obligaciones legales y estar en capacidad de evidenciar el correcto cumplimiento de sus deberes.

Con este principio se busca una realidad verificable en beneficio de la protección de los derechos de las personas.

DEBER DE SEGURIDAD.

Las personas titulares de los datos personales tienen derecho a que la información personal que proporcionen a todos los responsables, sean resguardados bajo medidas de seguridad adecuadas, que eviten su pérdida, alteración, destrucción, daño o uso, acceso o tratamiento no autorizado.

En ese sentido, los responsables estamos obligados a resguardar los datos personales en bases de datos protegidas con medidas de seguridad administrativas, físicas o técnicas.

- **Medidas administrativas:** Implementar controles que ayuden a evitar prácticas inadecuadas del personal que pongan en riesgo los datos personales, por ejemplo, evitar compartir contraseñas o dejar los expedientes al alcance de personas que no estén encargadas de su estudio o tramitación.
- **Medidas físicas:** Controles aplicados en los espacios físicos e infraestructura que minimicen el robo o acceso no autorizado, por ejemplo, mantener las áreas de trabajo, mobiliario y equipos debidamente cerrados con los controles y candados suficientes.
- **Medidas técnicas:** Controles para proteger equipos de cómputo y dispositivos de almacenamiento de virus, malware, entre otros.

DEBER DE CONFIDENCIALIDAD.

En artículo 25 de la LPDPPSOCHIS, refiere que toda persona tiene derecho a que sus datos personales sean tratados con confidencialidad, es decir, a que éstos no se difundan o compartan con terceros, salvo que exista consentimiento para ello o alguna obligación normativa requiera su difusión.

Ahora bien, sólo bajo ciertas circunstancias está permitida la comunicación de datos personales con terceros, principalmente si el titular de los mismos ha otorgado su consentimiento, pero también cuando se presente alguno de los siguientes supuestos:

- Cuando la transferencia esté prevista en una ley, convenios o Tratados Internacionales suscritos y ratificados por México;
- Cuando la transferencia se realice entre responsables del sector público, siempre y cuando los datos personales se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;

- Cuando la transferencia se realice a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable del sector privado, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas;
- Cuando la transferencia sea legalmente exigida para la investigación y persecución de los delitos, así como la procuración o administración de justicia;
- Cuando la transferencia sea necesaria para el reconocimiento, ejercicio o defensa de un derecho ante autoridad competente, siempre y cuando medie el requerimiento de esta última;
- Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios, siempre y cuando dichos fines sean acreditados;
- Cuando la transferencia sea requerida para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular;
- Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero, o
- Cuando la transferencia sea necesaria por razones de seguridad nacional.

Dicho lo anterior, se solicita considerar en el ámbito de su competencia, se dé cumplimiento a los principios y deberes que rigen la materia de protección de datos personales, a efecto de garantizar y proteger derechos de terceros.

5.- SISTEMA DE GESTIÓN DE LOS DATOS PERSONALES

Para el tratamiento de los datos personales que lleva a cabo el **H. Ayuntamiento de Totolapa, Chiapas**, garantiza el tratamiento de los datos personales que lleva a cabo como parte de sus funciones 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.



En este sentido, el **H. Ayuntamiento de Totolapa** 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. Por lo que se dio a la tarea facilitar un formato a las diferentes unidades administrativas, a realizar el levantamiento de inventarios de los datos personales que se encuentran bajo su responsabilidad, de acuerdo a lo establecido en el artículo 27 de la Ley de Protección de Datos Personales del Estado de Chiapas; esto, con el propósito de identificar entre otros aspectos, la categoría y tipo de datos que son sometidos a tratamiento, incluyendo los de carácter sensible; los medios a través de los cuales se obtienen dichos datos; el sistema físico y/o electrónico que se utiliza para su acceso, manejo, aprovechamiento, monitoreo y procesamiento; las características del lugar donde se ubican las bases físicas o electrónicas de datos; las finalidades del tratamiento, y el nombre, cargo y adscripción de los servidores públicos que tienen acceso 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.

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 Totolapa.

Una vez integrados los inventarios de tratamientos y de datos, se dispuso del 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:

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 excepciones 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 Totolapa;

- Respetar los derechos de los titulares en relación con sus datos personales;
- Identificar a los servidores públicos del Ayuntamiento de **Totolapa** responsables del tratamiento de los datos personales;

El **Ayuntamiento de Totolapa** 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 LGPDPSO y la LPDPPSOCHIS y los Lineamientos de la materia, siempre en consideración de la protección del derecho a la privacidad y protección de datos de las personas.

La identificación de vulnerabilidades y amenazas, se han establecido medidas de seguridad generales, de acuerdo con otras experiencias 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 lograr 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 LPDPSO de Chiapas y los lineamientos correspondientes.

6.- INVENTARIO DE TRATAMIENTOS Y DATOS PERSONALES

Para cumplir con los objetivos y obligaciones es necesario que cada una de las áreas administrativas identifiquen los procesos en los que actualmente se lleva a cabo tratamiento de datos personales; obteniendo con ello el **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 Totolapa**, 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:

- ✓ Secretario Municipal
- ✓ Juez Municipal



H. AYUNTAMIENTO MUNICIPAL CONSTITUCIONAL DE TOTOLAPA
2024-2027
UNIDAD DE TRANSPARENCIA



- ✓ Contralor Municipal
- ✓ Director de Obras Publicas
- ✓ Unidad de Transparencia
- ✓ DIF Municipal

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.

Unidad administrativa	Nombre y cargo de las y los Servidores Públicos que tratan Datos Personales	Actividades donde se recaban Datos Personales
Secretario Municipal	Miguel Angel Vazquez Lopez	*Atencion Ciudadana *Elaboración de Constancias
Juez Municipal	Antonia Hernandez Díaz	*Convenios y Asuntos Legales
Contralor Municipal	Edgali Hernandez Diaz	*Declaraciones Patrimoniales
Director de Obras	Wualter Ulises Moreno Lopez	*Registro de Contratistas y Proveedores
Unidad de Transparencia	Mario Vazquez Vazquez	*Solicitudes en General
DIF Municipal	Eulalia Lopez Gutierrez	*Apoyos en general

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

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, Menor de Edad, Nacionalidad, Nivel Educativo, Ocupación, Sexo, Teléfono fijo o Celular.

Patrimoniales

Número de Cuenta, Cuentas bancarias, estados de cuenta, CLABE interbancaria, institución bancaria, facturas, Descuentos personales.

Sensibles

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

Estos datos son utilizados en 1 procesos, de los cuales 2 corresponden a Secretaría Municipal, y de los demás uno a cada área siendo estas: Juez Municipal; Contralor Municipal; Director de Obras Públicas; Unidad de Transparencia y DIF Municipal.

7.- PROCESOS POR UNIDAD ADMINISTRATIVA

Como se puede apreciar la unidad administrativa con mayor número de procesos es Secretaría Municipal con 2 procesos, la mayoría tiene 1 proceso, las áreas enlistadas solicitan datos personales mientras que la Contraloría Municipal, es la única área que solicita datos patrimoniales, así mismo, en las áreas de Juez Municipal y DIF Municipal se utilizan datos sensibles.

A partir de la gráfica podemos verificar que los datos personales que más predominan son las de identificación ya que la mayoría de las áreas utilizan datos personales de carácter identificativo, en segundo término, los que incluyen datos patrimoniales y los datos sensibles los utiliza únicamente para un proceso.

Se logró identificar que las áreas tienen un medio diferente a las demás para obtener los datos personales, y estos son:

- ✓ Físicamente
- ✓ Correo electrónico
- ✓ 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 Totolapa, 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 Totolapa, 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 Totolapa, 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 y la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas 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.

Compromiso y Honestidad
que dan confianza

FUNCIONES Y RESPONSABILIDADES DEL TRATAMIENTO DE DATOS PERSONALES

A continuación, se ilustran las funciones otorgadas a quienes llevan a cabo tratamientos de datos personales.

Unidad administrativa	Nombre y cargo de las y los Servidores Públicos que tratan Datos Personales	Actividades donde se recaban Datos Personales
Secretario Municipal	Miguel Angel Vazquez Lopez	*Atención Ciudadana *Elaboración de Constancias
Juez Municipal	Antonia Hernandez Diaz	*Convenios y Asuntos Legales
Contralor Municipal	Edgali Hernandez Diaz	*Declaraciones Patrimoniales
Director de Obras	Wualter Ulises Moreno Lopez	*Registro de Contratistas y Proveedores
Unidad de Transparencia	Mario Vazquez Vazquez	*Solicitudes en General
DIF Municipal	Eulalia Lopez Gutierrez	*Apoyos en general

8.- PROGRAMA DE TRABAJO PARA LA IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD

Sección Clasificada del Documento de Seguridad, apartado **Programa de Trabajo para la Implementación de Medidas de Seguridad**.

Se testa el apartado número 9, que contiene el Programa 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

9.- ANÁLISIS 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.

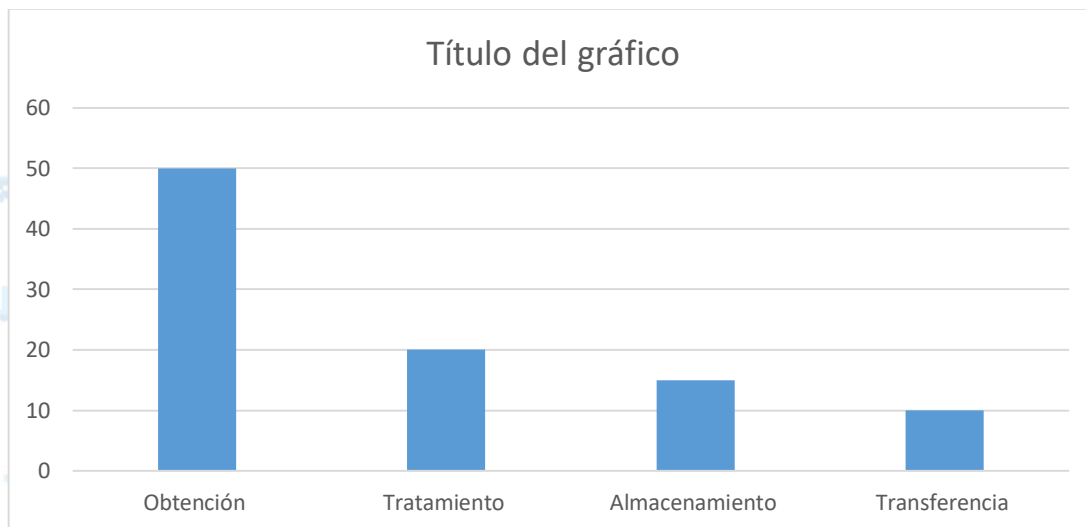
10.- ANÁLISIS DE LA INFORMACIÓN

El H. Ayuntamiento de Totolapa cuenta con 6 áreas administrativas en las que tiene lugar datos personales para el desarrollo de los 7 procesos que se ilustran a continuación:

Áreas Administrativas	Procesos
Secretario Municipal	2
Juez Municipal	1
Contralor Municipal	1
Director de Obras Públicas	1
Unidad de Transparencia	1
DIF Municipal	1
Total	7

En consecuencia, es H. Ayuntamiento para la obtención, tratamiento, almacenamiento, transferencia, de los datos y en el que se encuentra más vulnerable es en el periodo de obtención en un 50%; mientras que el periodo que implica menor riesgo es el de transferencia con un 10%.

Frecuencia de riesgo por la etapa de ciclo de vida



Las amenazas a las que se ven expuestos son básicamente:

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

Siendo la más alta, la de robo, y la de menor riesgo es daño, alteración o modificación no autorizada.

Asimismo, los datos personales corresponden a menos de 300 personas, lo que reduce el nivel de riesgo y se mantienen a resguardo.

11.- MEDIDAS DE SEGURIDAD

Las medidas de seguridad administrativas, físicas y técnicas que actualmente se aplican en este H. Ayuntamiento para mantener la confidencialidad e integridad de la información, es de manera que solo personal autorizado puede tener acceso a los datos personales así mismo impedir la divulgación no autorizada, son las siguientes:

a) Medidas administrativas

Capacitación permanente en materia de la Ley de Protección de Datos Personales en posesión de Sujetos Obligados del Estado de Chiapas (LPDPPSOCHIS), impartido a quienes colaboran en este H. Ayuntamiento de Totolapa.

b) Medidas físicas

Protección de documentos e información resguardándolos en archivos físicos de trámite y concentración, asegurados con llave.

c) Medidas técnicas

1. Garantizar la seguridad de los datos personales, utilizando claves de usuario y contraseñas de manera individual y evitar compartirlas.
2. Mantener los documentos electrónicos y físicos en lugares seguros, bajo llave, dentro de cajones cerrados, o bajo la protección de alguna contraseña, a fin de restringir el acceso a los datos personales que pudieran mantenerse en archivos y equipos.
3. Cuidar que en los equipos de impresión no se dejen olvidados documentos que contengan datos personales.

12.- MONITOREO DE MEDIDAS DE SEGURIDAD

Como parte del programa de protección de datos personales, es importante la supervisión de las medidas de seguridad técnicas y físicas, como vigilar que el ingreso de personas sea a través de los accesos correspondientes, plenamente identificados e incluso ser verificadas por el oficial de datos personales.

1. Revisión y actualización permanente de las contraseñas utilizadas para resguardar los datos personales en equipos de cómputo.
2. Revisar de manera permanente el cumplimiento de protocolos implementados para la protección de los datos personales.
3. Vigilar que el ingreso de personas sea a través de los accesos correspondientes, plenamente identificados.

13.- PROPUESTA DE CAPACITACIÓN EN MATERIA DE DATOS PERSONALES

La aplicación del programa de protección de datos personales en el H. Ayuntamiento Municipal de Totolapa se rige por los mecanismos que maneja, Transparencia para el



H. AYUNTAMIENTO MUNICIPAL CONSTITUCIONAL DE TOTOLAPA
2024-2027
UNIDAD DE TRANSPARENCIA



Pueblo de Chiapas, 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,

Es así como este H. Ayuntamiento cumple en cuanto a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados, esto con la finalidad de Impulsar la implementación de esquemas de mejores prácticas que fortalezcan la protección de los datos, con base en las disposiciones previstas en la normativa aplicable.

A manera de propuesta, se han considerado los siguientes temas:

I) Ley de protección de datos personales en posesión de sujetos obligados en Chiapas	II) Obligaciones en la observancia de la LPDPPSOCHIS	III) El programa de protección de datos personales	IV) Avisos de Privacidad en el marco del programa de protección de datos personales
*Importancia y evolución de Ley de Datos Personales.	• Medidas de seguridad. • Procedimientos y sanciones/ Derechos ARCO • Medios de defensa.	• Sistemas de datos personales. • Inventario y Base de Datos. • Medidas de seguridad. • Análisis de brecha y de riesgo.	• Contenido: Integral, simplificado • Consentimiento. • Deber de información.