

DOCUMENTO DE SEGURIDAD

DIF MUNICIPIO DE TILA, CHIAPAS

Índice

Introducción	3
Objetivos y alcances	4
• Objetivo general	
• Objetivos específicos	
• Alcance del documento	
Datos personales	5
• Catálogo de medios físicos y electrónicos a través de los cuales se obtienen Los datos personales.	
• Ubicación de los datos personales	
• Quienes tienen permiso de acceso o manejo de los datos personales	
• Transferencia de los datos personales	
• Plazo de conservación	
Sistema de gestión de seguridad de los datos personales	7
Inventario de datos personales y de los sistemas de tratamiento	12
Funciones y Obligaciones de las personas que tratan datos personales	13
Análisis de riesgo y brecha	17

- Análisis de riesgo
- Análisis de brecha

Gestión de vulneración y plan de contingencia	25
• Gestión de vulneración • Plan de contingencia	
Medidas de seguridad general	32
• Medidas de seguridad administrativas • Medidas de seguridad físicas • Medidas de seguridad técnicas	
Plan de trabajo	34
Programas de capacitación en materia de protección de datos personales	36
Marco jurídico.	38

1.- INTRODUCCION:

El DIF municipal de Tila, Chiapas, tiene a bien elaborar el siguiente documento de seguridad con la finalidad de garantizar la confidencialidad, integridad y disponibilidad de los datos personales, a través de las medidas de seguridad diseñadas por el sujeto obligado que los posee, debiendo de observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad.

Así como también cumpliendo estrictamente con relación a los artículos 6 y 16 de la constitución política de los estados unidos mexicanos, la ley general de protección de datos personales en posesión de sujetos obligados, ley de protección de datos personales en posesión de sujetos obligados del estado de Chiapas, se considerara que la información recabada a través de los departamentos que conforman la estructura del sujeto obligado en este caso del DIF del municipio de Tila debe de ser protegida a través de la implementación de procesos administrativos e informáticos que permitan la administración de datos personales recabados como parte de las atribuciones y facultades conferidas, y con la finalidad, de garantizar el derecho de cada persona a la protección de sus datos personales en posesión del sujeto obligado.

Dicho lo anterior, el presente documento se integra a partir de la gestión de actividades coordinadas orientadas a controlar y verificar que el tratamiento de los datos personales se lleve a cabo conforme a los principios y deberes que rigen la materia. En este sentido, para DIF del municipio de Tila, Chiapas, la política de seguridad de los datos personales constituye un compromiso permanente con el cumplimiento de las disposiciones previstas tanto en la legislación general como en la normativa local aplicable.

Para tal efecto, y en términos de lo dispuesto por el artículo 29 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, que establece la obligación de los responsables de elaborar su Documento de Seguridad como parte de un proceso de mejora continua, el DIF del municipio de Tila, Chiapas; ha llevado a cabo diversas acciones orientadas a su creación.

Entre dichas acciones destacan la elaboración de los inventarios de datos personales, la revisión y fortalecimiento de las medidas de seguridad implementadas para su

tratamiento, así como la realización de análisis de riesgos y de brecha, con el propósito de monitorear la eficacia de las medidas adoptadas, identificar posibles vulnerabilidades y mitigar los riesgos asociados al tratamiento de datos personales.

Asimismo, se ha impulsado un proceso permanente de sensibilización institucional sobre la importancia de adoptar medidas preventivas y correctivas en la materia, tomando como referencia los resultados obtenidos de la revisión de los sistemas de datos personales, así como los esquemas de autorregulación y capacitación del personal, con el fin de fortalecer la protección de la información bajo resguardo del DIF del municipio de Tila, Chiapas.

2.- OBJETIVOS Y ALCANCE DEL DOCUMENTO.

OBJETIVO GENERAL.

Elaborar un documento de seguridad que brinde certeza en el tratamiento de los datos personales resguardado en la dirección del DIF del municipio, con el fin de proteger los datos personales en posesión del DIF del municipio de Tila.

OBJETIVOS ESPECIFICOS.

Así como también tiene a bien emitir el presente documento de seguridad con dos subjetivos los cuales radican en:

1. Proveer el marco de trabajo necesario para la protección de los datos personales en posesión de este sujeto obligado para garantizar su seguridad.
2. Establecer los mecanismos de dirección, operación y control de los procesos que implique el manejo de datos personales, a efecto de protegerlos de manera segura toda información.

ALCANCE DEL DOCUMENTO:

El presente Documento de Seguridad estará disponible para todos y cada uno de los departamentos que conforman el DIF del municipio de Tila, y que, en el ejercicio de sus atribuciones, recaben, administren, transfieran o manejen bases de datos, así como también aquellos datos que obren en soportes físicos o electrónicos.

Lo anterior conforme a lo establecido en la LGPDPPSO y la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas y los Lineamientos para la Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Chiapas.

3.- DATOS PERSONALES

Los departamentos correspondientes al DIF del municipio de Tila, recabara para las finalidades antes señaladas, una serie de datos personales no sensibles, los cuales son los siguientes:

- Nombre y apellido
- Sexo
- Correo electrónico
- Teléfono celular y/o fijo
- Entidad federativa
- Institución a la que pertenece
- Cargo dentro de la institución
- Indicar si es integrante de algún sindicato de trabajadores u organización.
- Ultimo grado académico
- Título profesional
- Cedula profesional
- Diciplina y campo de estudio.

catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales, son los siguientes:

Directamente del titular:

1. Teléfono fijo
2. Teléfono móvil
3. Correo electrónico
4. Formularios electrónicos
5. Cuestionarios impresos

Ubicación de los datos personales

Con base en el artículo 63 de la ley general de protección de datos personales en posesión de sujetos obligados (LGPDPPSO), los datos personales en formato digital se resguardan en la infraestructura de cómputo y en la nube; los datos personales en formato físico se resguardan en el archivo correspondiente a la Dirección del DIF del municipio, ubicado en las instalaciones que ocupa el edificio del DIF municipal.

Quienes tienen permiso de acceso o manejo de los datos personales:

Solamente el personal adscrito y autorizado al DIF del municipio de Tila, Chiapas y con los permisos habilitados puede tener acceso y manejo de datos personales resguardados.

Trasferencia de datos personales:

Se podrán realizar transferencia a entes públicos y/o autoridades competentes en todos aquellos requerimientos debidamente fundados y motivados para las finalidades requeridas.

Para los fines delimitados anteriormente, no se omite mencionar que no requerirán de su consentimiento, de conformidad con los artículos 70, fracciones II, IV y VI de la de la ley general de protección de datos personales en posesión de sujetos obligados LGPDPPSO.

Plazo de conservación:

5 años

4.- SISTEMA DE GESTION DE SEGURIDAD DE LOS DATOS PERSONALES EN POSESION DEL DIF DEL MUNICIPIO DE TILA, CHIAPAS.

Para el tratamiento de los datos personales que lleva a cabo el DIF del municipio de Tila Chiapas, mediante su obtención, uso, registro, organización, conservación, acceso, manejo, aprovechamiento, transferencia, disposición o cualquier otra operación aplicable, se establecen políticas, procedimientos y mecanismos de seguridad orientados a garantizar su confidencialidad, integridad y disponibilidad.

Lo anterior se realiza en estricto apego a los principios, deberes y obligaciones previstos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la Ley General de Transparencia y Acceso a la Información Pública, la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas y la Ley de Transparencia y Acceso a la Información Pública del Estado de Chiapas, así como demás disposiciones normativas aplicables en la materia.

En tal virtud, el DIF del municipio de Tila, Chiapas, inició su proceso de planificación de los esquemas de protección de datos mediante la identificación de todos y cada uno de los procesos y tareas en los que, de acuerdo con el ámbito de funciones de las distintas áreas que conforman el municipio de Tila, se involucra el tratamiento de datos personales. Para ello, se dispuso de un formato que permitió a los diversos órganos administrativos realizar el levantamiento de inventario de los datos personales que se encuentran bajo su responsabilidad, considerando los elementos mínimos que establece el artículo 27 de Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas y el artículo 53 de los Lineamientos para la Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Chiapas.

Es así que a través del desarrollo de un instrumento estandarizado, se llevó a cabo el levantamiento de inventario de datos, 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, el nombre, cargo y adscripción de los servidores públicos que tienen acceso a los datos personales, 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; y la vía útil de los datos personales, en ese mismo sentido, el inventario ha contribuido desde el punto operativo a considerar el ciclo de vida de los datos personales, de forma tal que los servidores públicos que intervienen en el tratamiento conocen que, una vez concluida la finalidad los datos, estos 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 de la Institución.

De igual forma, una vez integrados los inventarios de datos, se dispuso de la metodología para la elaboración del análisis de riesgos, en la cual, atendiendo a lo previsto en el artículo 27, fracción IV de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas, las áreas responsables de su tratamiento identificaron el valor de los datos personales de acuerdo con su categoría y el ciclo de vida; el valor de exposición de los activos involucrados en el tratamiento; las consecuencias que pueden generarse para los titulares de los mismos con motivo de su posible vulneración y, los factores de riesgo a los que eventualmente se encuentran expuestos.

Con base en dicho análisis de riesgo, además de promover el reconocimiento de las medidas de seguridad administrativas, entendidas como el conjunto de políticas y procedimientos de gestión, soporte y revisión de la seguridad de la información; físicas, que corresponden a las acciones o mecanismos para proteger el entorno físico de los datos, así como de los recursos involucrados en su tratamiento y, técnicas que se valen

de la tecnología para proteger el entorno digital de la información, también se ha identificado 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:

DIAGRAMA



Considerando que 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.

Aunado a las anteriores vulnerabilidades, de manera enunciativa mas no limitativa, se examinan algunos tipos de amenazas, que pueden ser intencionales o no, a las que podría enfrentarse la institución y sus activos de información.

Tipo de amenazas

- Robo, extravió o copia no autorizada
- Uso, acceso o tratamiento no autorizado
- Daño, alteración o modificación no autorizada
- Perdida o destrucción no autorizada
- Entre otras.

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 con el fin de comprometer 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 vulnerabilidades y amenazas, se han establecido medidas de seguridad generales, que de acuerdo a la experiencia y mejores prácticas son monitoreadas para lograr la mejora continua por parte de todos los involucrados en el tratamiento. Como parte del sistema de gestión y política de seguridad institucional, se enmarcan las políticas y procedimientos generales, mismas que se desarrollan en el presente documento.

En base en lo anterior, el DIF del municipio de Tila, Chiapas; determina las líneas de acción del personal encargado de tratamiento de datos personales con el propósito de generar su correcto resguardo, buscando en todo momento actuar en apego a las directrices de la legislación vigente y los Lineamientos de la materia establecen, siempre en consideración de la salvaguarda del derecho a la privacidad y protección de datos de las personas.

5.- INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO DEL MUNICIPIO DE TILA, CHIAPAS

Del inventario de datos personales, deriva los procesos que realizan las áreas que integran el DIF del municipio de Tila, Chiapas, con motivo de los datos que se recaban de las personas, a través del ejercicio de sus funciones, 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 estos derechos.

Las categorías de datos personales tratados en el DIF del municipio de Tila, Chiapas; son las siguientes:

De identificación:

Nombre, domicilio, C.U.R.P., fotografía, huella digital, firma, edad, clave de elector, estado civil R.F.C., correo electrónico personal, teléfono, sexo, información académica, fecha y lugar de nacimiento, cédula profesional, nacionalidad, número de pasaporte, número de licencia de conducir, número de placa de vehículo, número de seguridad social.

Patrimoniales:

Cuentas bancarias, estados de cuentas bancarias, número de tarjeta bancaria, CLABE interbancaria, Institución bancaria, facturas, estados financieros, información fiscal, información fiduciaria, información financiera, saldos, propiedades, pensión alimenticia, descuentos por concepto de primas de seguro.

Sensibles:

Diagnóstico médico, antecedentes médicos, tipo de sangre, datos biométricos, antecedentes penales y resultados de evaluación psicométrica y de valores.

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

La ley general de protección de datos personales en posesión de sujetos obligados (LGPDPPSO) tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de datos personales, en posesión de sujetos obligados.

El derecho a la protección de datos personales solamente se limitará por razones de interés público y seguridad nacional, en términos del artículo 6 de la ley general de protección de datos personales en posesión de sujetos obligados (LGPDPPSO).

La ley general de protección de datos personales en posesión de sujetos obligados (LGPDPPSO) aplica a cualquier tratamiento de datos personales que obren en soportes físicos o electrónicos, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización de conformidad con el artículo 4.

Por regla general NO podrán tratarse datos personales SENSIBLES, salvo que se cuente con el consentimiento expreso de su titular o en su defecto, se trate de los casos establecidos en el artículo. 22 de la ley general de protección de datos personales en posesión de sujetos obligados (LGPDPPSO).

Los responsables del tratamiento de datos personales deberán observar los principios de licitud, finalidad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales.

Todo tratamiento de datos personales que efectúe el responsable deberá estar justificado por las finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que

la normatividad aplicable le confiere.

El responsable de establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

El tratamiento de los datos personales con motivo de las finalidades previstas en el presente documento, no requerirán de su consentimiento expreso, de conformidad con lo establecido en el artículo 22, fracciones IV y V de la ley general de protección de datos personales en posesión de sujetos obligados (LGPDPPO).

FUNCIONES Y OBLIGACIONES PARA EL TRATAMIENTO DE DATOS PERSONALES DEL DIF MUNICIPIO DE TILA, CHIAPAS.

RESPONSABLES	• DIF del municipio de Tila, Chiapas. • Comité de transparencia • Unidad de transparencia municipal
FUNCIONES	• Actualizar la base de datos de integrantes de los departamentos del DIF de municipio de Tila, para mantener la comunicación institucional y brindar asesorías sobre su operación • Conformar una base de datos sobre especialistas financieros, con el propósito de contar con información sobre las áreas de conocimiento y especialización de los integrantes de los departamentos del DIF del municipio de Tila, para desarrollar actividades de capacitación • Difundir el perfil operativo de los departamentos del DIF del municipio de Tila y sus datos de contacto para las personas interesadas en la cuenta pública y público en general que desee contactarlas • Otorgar el acceso exclusivo a plataformas electrónicas para actividades educativas dirigidas a los

	departamentos del DIF del municipio de Tila y personas interesadas, con el fin de asegurar el ingreso, la posterior emisión de constancias electrónicas. • Generar diagnósticos sobre la operatividad de los departamentos del DIF del municipio de Tila, en cuanto a sus intereses de capacitación, avances y dificultades en el cumplimiento de sus funciones y vinculación con instituciones afines.
OBLIGACIONES	• De acuerdo a lo dispuesto por el artículo 21 de la ley general de protección de datos personales en posesión de los sujetos obligados (LGPDPSSO), el DIF del municipio de Tila, Chiapas., en el marco de sus obligaciones debe contar con el consentimiento tácito o expreso del titular para el tratamiento de sus datos personales. • Realizar el tratamiento de los datos personales conforme a las instrucciones del responsable y las señaladas en la normatividad aplicable • Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable y las señaladas en la normatividad aplicable en la materia de recursos humanos. • Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables • Informar al responsable cuando ocurra una vulneración a los datos personales que trata por sus instrucciones. • Guardar confidencialidad respecto a los datos personales tratados • Suprimir o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales.

	• Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
DATOS CONTENIDOS EN LOS FORMULARIOS ELECTRONICOS Y EN LOS FORMATOS IMPRESOS DE SOLICITUD DE DATOS	Los formularios electrónicos y en los formatos impresos de solicitud de datos puede contener DATOS PERSONALES NO SENSIBLES, tales como: • Nombre y apellido • Entidad federativa • Correo electrónico • Teléfono fijo y/o celular • Instituciones a las que pertenece • Cargo dentro de la institución • Si es integrante de algún sindicato u organización. • Último grado de estudio Los DATOS PERSONALES antes descritos pueden estar contenidos en los requisitos para presentar su solicitud que incluyen: • Formatos para capacitaciones, eventos y actividades en cuenta pública. • Formulario de reuniones virtuales con dependencias de gobierno. • Formulario para la actualización anual de perfiles y directorio del sujeto obligado.

7.- ANALISIS DE RIESGO Y BRECHA.

ANALISIS DE RIESGO

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo y Brecha.

Se testa el apartado número 7, 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 7, 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

ANÁLISIS DE BRECHA

Sección Clasificada del Documento de Seguridad, apartado del Análisis de Riesgo y Brecha.

Se testa el apartado número 7, 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 7, 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 7, 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 7, 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 7, 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 7, 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 7, 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 7, 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

8.- GESTION DE VULNERACIONES Y PLAN DE CONTINGENCIA

Sección Clasificada del Documento de Seguridad, apartado de Gestión y Plan de Contingencia.

Se testa el apartado número 8, 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 de Gestión y Plan de Contingencia.

Se testa el apartado número 8, 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 de Gestión y Plan de Contingencia.

Se testa el apartado número 8, 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 de Gestión y Plan de Contingencia.**

Se testa el apartado número 8, 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 de Gestión y Plan de Contingencia.

Se testa el apartado número 8, 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 de Gestión y Plan de Contingencia.

Se testa el apartado número 8, 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 de Gestión y Plan de Contingencia.

Se testa el apartado número 8, 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.

9.- TIPOS DE MEDIDAS DE SEGURIDAD:

1. **Medidas de seguridad administrativas:** políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel dirección, mediante la identificación, clasificación y borrado seguro de la información; así como la sensibilización y capacitación del personal, en materia de protección de datos personales.
2. **Medidas de seguridad físicas:** conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. Por lo que se deben considerar las siguientes actividades:
 - Prevenir el acceso no autorizado al perímetro del departamento, sus instalaciones físicas, áreas críticas, recursos e información.
 - Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de los departamentos, recursos e información.
 - Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de las instalaciones de los departamentos del DIF del municipio de Tila, Chiapas.
 - Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad
3. **Medidas de seguridad técnicas:** conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. Por lo que, se deben considerar las siguientes actividades:
 - Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados.
 - Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones
 - Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware.
 - Gestionar las comunicaciones, operaciones y medios de almacenamiento de los

recursos informáticos en el tratamiento de datos personales.

MEDIDAS DE SEGURIDAD A IMPLEMENTAR

Además de las medidas de seguridad ya establecidas en cada área, se plantea implementar las siguientes medidas de seguridad:

MEDIDAD A IMPLEMENTAR	TIPO DE MEDIDAS
1.- Clasificación y control de activos: establecer los controles en materia de identificación, inventario, clasificación y valuación de los activos conforme a la normatividad aplicable	Administrativa
2.- seguridad relacionada a los recursos humanos: el personal deberá conocer el alcance de sus responsabilidades respecto a la seguridad de activos antes, durante y al finalizar la relación laboral.	Administrativa
3.- términos y condiciones de empleo: se deberá establecer los términos o condiciones de confidencialidad, de acuerdo con el tratamiento y responsabilidad de los datos personales que obran en cada area.	Administrativa
4.- seguridad física y ambiental: establecer los controles relacionados con los perímetros de seguridad física y el entorno ambiental de los activos con el fin de prevenir accesos no autorizados, daño, robo, entre	Física

otros. Espacios seguros y seguridad de equipo	
5.- colocar aviso de "solo personal autorizado"	Física
6.- Registro en bitácora de los solicitantes de la información	Física
7.- sensibilidad y capacitación: fomentar en los servicios públicos la seguridad de la información y recibir capacitación de manera periódica respecto al tratamiento que realicen de los datos personales	Administrativa
8.- establecer contraseñas: implementar contraseñas para toda la información que se tiene resguardada en los equipos de cómputo y medios electrónicos.	Técnica

10.- PLAN DE TRABAJO.

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

Se testa el apartado número 10, 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 Chiapas, así como en el artículo trigésimo octavo de lineamientos generales en materia de clasificación y descalificación de la información, así como para la elaboración de versiones publicas.

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

Se testa el apartado número 10, 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 Chiapas, así como en el artículo trigésimo octavo de lineamientos generales en materia de clasificación y descalificación de la información, así como para la elaboración de versiones publicas.

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

Se testa el apartado número 10, 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 Chiapas, así como en el artículo trigésimo octavo de lineamientos generales en materia de clasificación y descalificación de la información, así como para la elaboración de versiones publicas.

11.- PROGRAMA GENERAL DE CAPACITACION INSTITUCIONAL

En el marco normativo de la ley general de protección de datos personales en posesión de sujetos obligados, la ley federal de transparencia y acceso a la información pública y demás ordenamientos aplicables en materia, el DIF del municipio de Tila, Chiapas., estableció un programa de capacitaciones para su personal, en relación con la protección de datos personales que recaba de terceros, como parte sus actividades, para el logro de objetivos institucionales,

El objetivo del programa de capacitación es que el personal del DIF del municipio de Tila, Chiapas., conozca la normatividad respecto del tratamiento de datos personales de terceros en posesión de sujetos obligados así como las políticas establecidas por el responsable respecto de las funciones y obligaciones de las personas que tratan este tipo de datos, los mecanismos de monitoreo y las medidas de seguridad implementadas, el inventario de datos personales y su tratamiento y el análisis de brecha y riesgo, para tener los elementos necesarios y aplicar dichas políticas en sus actividades.

Dicho programa se aplicara en tres etapas:

- 1.- Una primera etapa, incluye la detección de necesidades de capacitación para identificar el nivel y tipo de capacitación para el personal para llevar a cabo la capacitación a todo el personal del DIF del municipio de Tila, respecto a la ley federal de transparencia y acceso a la información pública y la ley general de protección de datos personales en posesión de sujetos obligados. Estos cursos serán impartidos por el comité de transparencia o el responsable de la unidad de transparencia del DIF del municipio de Tila, y son de carácter obligatorio para todo el personal.
- 2.- Una segunda etapa en la que se da a conocer, la normatividad vigente en materia de protección de datos personales, las consecuencias del incumplimiento de los requerimientos legales, el uso de herramientas tecnológicas utilizadas para el tratamiento de datos personales y para la implementación de medidas de seguridad, el documento de seguridad y el o los avisos de privacidad con el objeto de que conozca los procedimientos establecidos por el comité para el manejo y tratamiento de los datos que recaba, las medidas de seguridad implementadas, los riesgos en el manejo de los datos y que medidas preventivas se debe aplicar, tipo de datos que se manejan, quienes son los encargados de recabar, resguardar y tratar.
- 3.- Una tercera etapa que consistirá en capacitar al personal que se encarga y maneja los datos de terceros; esta capacitación se llevara a cabo a través de los recursos de capacitación especializada que se puedan obtener, con la finalidad de que dicho personal tenga mayores elementos y herramientas en el manejo de los datos de terceros y dar así cumplimiento a lo establecido en la normatividad aplicable para esto.

12.- MARCO JURÍDICO

Para efectos del cumplimiento y elaboración del presente documento, las disposiciones legales aplicables son:

- Constitución Política de los Estados Unidos Mexicanos.
- Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados.
- Constitución Política del Estado Libre y Soberano de Chiapas.
- Ley Orgánica de la Administración Pública para el Estado de Chiapas.
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas.
- Lineamientos para la protección de datos personales en posesión de sujetos obligados para el estado de Chiapas

DOCUMENTO DE SEGURIDAD		
SISTEMA DE DATOS PERSONALES MUNICIPIO DE TILA, CHIAPAS		
	Fecha de Elaboración del Documento de Seguridad: 28 de SEPTIEMBRE 2026.	Fecha de Última Actualización del Documento de Seguridad: 28 de SEPTIEMBRE 2026.
	Elaboró: C.P. JUAN DIEGO CRUZ ALFARO Unidad de Transparencia.	Aprobó: C. LALILA MIRIAM CRUZ CRUZ DIRECTOR DEL DIF MUNICIPAL