"EN PRO DE LA SEGURIDAD SOCIAL"

DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES DEL SINDICATO UNICO DE TRABAJADORES AL SERVICIO DEL MUNICIPIO DE ATITALAQUIA HIDALGO. (S.U.T.S.M.A.H.)

SINDICATO UNICO DE TRABAJADORES AL SERVICIO DEL MUNICIPIO DE ATITALAQUIA, HIDALGO.

DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES

S.U.T.S.M.A.H

T.P.S.E. Cleotilde Elizabeth Juárez Cruz
Secretaria General del S.U.T.S.M.A.H.

Arq. Itaik Onofre Badillo
Encargado de Transparencia
del S.U.T.S.M.A.H

CONTENIDO

INTRODUCCIÓN.....04

OBJETIVOS.....05

OBJETIVOS GENERALES Y ESPECÍFICOS DEL DOCUMENTO DE SEGURIDAD....05

CONCEPTOS BÁSICOS.....06

RESPONSABILIDADES.....09

MARCO NORMATIVO.....09

SISTEMAS DE GESTIÓN DE DATOS PERSONALES.....10

CATÁLOGO, DESCRIPCIÓN Y MEDIDAS DE SEGURIDAD DE LOS SISTEMAS DE DATOS PERSONALES DEL S.U.T.S.M.A.H.....11

CONTROLES Y MECANISMOS DE SEGURIDAD.....13

LAS BITÁCORAS DE ACCESO, OPERACIÓN COTIDIANA Y VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES.....14

ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA.....17

GESTIÓN DE VULNERACIONES.....17

MEDIDAS DE SEGURIDAD APLICADAS A LAS INSTALACIONES.....13

LOS PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES.....19

EL PLAN DE TRABAJO Y PROGRAMA GENERAL DE CAPACITACIÓN.....20

MECANISMOS DE MONITOREO Y REVISIÓN DE MEDIDAS DE SEGURIDAD.....20

CONCLUSIONES.....21

INTRODUCCIÓN

En los últimos años, la protección de los datos personales ha adquirido una importancia fundamental para garantizar la privacidad, la seguridad y el respeto a los derechos de las personas. En un contexto caracterizado por el uso creciente de medios electrónicos y el intercambio constante de información, resulta indispensable establecer medidas y procedimientos que permitan asegurar que los datos personales sean tratados de manera responsable, legítima y segura, evitando su pérdida, alteración, destrucción, uso, acceso o divulgación no autorizados.

El derecho a la protección de los datos personales constituye un derecho humano reconocido en la Constitución Política de los Estados Unidos Mexicanos, particularmente en sus artículos 6.º y 16, así como en las disposiciones legales aplicables en la materia. Su observancia implica la adopción de principios, deberes y medidas orientados a garantizar que el tratamiento de la información personal se realice conforme a la normativa vigente, respetando la privacidad de sus titulares y salvaguardando sus derechos.

En este sentido, el Sindicato Único de Trabajadores al Servicio del Municipio de Atitalaquia, Hidalgo **(S.U.T.S.M.A.H.),** reconoce la importancia de proteger los datos personales que se encuentran bajo su posesión y tratamiento, particularmente aquellos relacionados con sus agremiados, representantes, trabajadores y demás personas con quienes mantiene una relación institucional. La información contenida en expedientes, registros administrativos, documentación laboral y sindical, así como en los medios físicos y electrónicos utilizados para el desarrollo de sus actividades, requiere de medidas adecuadas que permitan preservar su confidencialidad, integridad y disponibilidad.

Por lo anterior, y en atención a la necesidad de fortalecer las prácticas institucionales en materia de protección de datos personales se elabora el presente Documento de Seguridad para la Protección de Datos Personales, como instrumento destinado a identificar, documentar y orientar la implementación de las medidas de seguridad administrativas, físicas y técnicas necesarias para proteger la información personal durante todo su ciclo de vida, desde su obtención y utilización hasta su conservación, bloqueo o supresión, según corresponda.

El presente documento tiene como propósito establecer una base de referencia para identificar los tratamientos de datos personales, las áreas y personas que intervienen en ellos, los sistemas y medios utilizados para su manejo, los riesgos y vulnerabilidades asociados, así como las medidas de seguridad existentes y aquellas que deban fortalecerse o implementarse. Asimismo, busca contribuir a la definición de responsabilidades, la prevención y atención de incidentes de seguridad, la capacitación del personal involucrado y la mejora continua de los procedimientos relacionados con el tratamiento de datos personales.

Para alcanzar estos objetivos, resulta indispensable observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, en los términos que establezca el marco jurídico aplicable, así como atender los deberes de seguridad y confidencialidad. La aplicación de estos principios y deberes permite orientar

las actuaciones institucionales hacia un manejo responsable de la información y reducir los riesgos derivados de su acceso, utilización o divulgación indebidos.

La elaboración de este instrumento constituye un proceso de identificación, diagnóstico y fortalecimiento institucional. Por ello, su contenido deberá sustentarse en información verificable sobre las condiciones reales de operación del Sindicato, distinguiendo las medidas de seguridad cuya existencia haya sido comprobada de aquellas que se encuentren pendientes de diagnóstico, validación, formalización o implementación. Esta distinción permitirá establecer acciones de mejora acordes con las necesidades institucionales y dar seguimiento a su cumplimiento.

En consecuencia, el Documento de Seguridad para la Protección de Datos Personales representa una herramienta de referencia para promover una cultura de responsabilidad, prevención y protección de la información dentro del S.U.T.S.M.A.H., fortalecer la confianza de sus agremiados y de las personas cuyos datos sean tratados por la organización, y contribuir al cumplimiento de las obligaciones que resulten aplicables en esta materia.

Su contenido deberá mantenerse actualizado conforme se identifiquen nuevos tratamientos de datos personales, se verifiquen las medidas existentes, se determinen las acciones necesarias y se produzcan cambios en los procedimientos, sistemas o disposiciones jurídicas aplicables, con el propósito de favorecer una protección efectiva, continua y documentada de los datos personales.

OBJETIVOS

1.- Objetivo General

Establecer un instrumento institucional que permita identificar, documentar, evaluar y fortalecer las medidas de seguridad aplicables al tratamiento de los datos personales en posesión del Sindicato Único de Trabajadores al Servicio del Municipio de Atitalaquia, Hidalgo (S.U.T.S.M.A.H.), mediante la identificación de los tratamientos de información, las responsabilidades de las personas involucradas, los riesgos y vulnerabilidades existentes, así como las medidas administrativas, físicas y técnicas necesarias para proteger los datos personales, preservar su confidencialidad, integridad y disponibilidad, y contribuir al cumplimiento de las disposiciones jurídicas aplicables.

2.- Objetivos específicos

1. **Identificar y documentar los tratamientos de datos personales** realizados por el Sindicato, incluyendo los tipos de datos recabados, sus finalidades, los medios de obtención, almacenamiento, consulta, utilización y conservación, así como las áreas y personas que intervienen en dichos procesos.
2. **Determinar las medidas de seguridad existentes** para la protección de los datos personales, mediante la revisión de los procedimientos, controles administrativos, espacios físicos, equipos de cómputo, cuentas de usuario y medios electrónicos utilizados para el manejo de la información.
3. **Identificar y evaluar los riesgos y vulnerabilidades** que puedan comprometer la confidencialidad, integridad o disponibilidad de los datos personales, considerando las condiciones reales de operación del Sindicato y las características de la información que administra.

4. **Establecer acciones de mejora y medidas de seguridad** de carácter administrativo, físico y técnico, orientadas a prevenir accesos no autorizados, pérdida, alteración, destrucción o divulgación indebida de datos personales.
5. **Definir responsabilidades y mecanismos de control** para las personas que, en el ejercicio de sus funciones, tengan acceso a datos personales, promoviendo su manejo responsable y el cumplimiento de los deberes de confidencialidad y seguridad correspondientes.
6. **Establecer procedimientos de atención y respuesta ante incidentes de seguridad**, así como mecanismos para su identificación, documentación, comunicación y seguimiento, conforme a las obligaciones que resulten aplicables.
7. **Promover la capacitación y sensibilización** de las personas involucradas en el tratamiento de datos personales, con el propósito de fortalecer las prácticas institucionales de protección y reducir los riesgos derivados de errores, descuidos o actuaciones no autorizadas.
8. **Implementar mecanismos de seguimiento, revisión y actualización** del Documento de Seguridad, a fin de mantenerlo congruente con los tratamientos de datos personales, las medidas de seguridad verificadas, los cambios operativos y las disposiciones jurídicas aplicables.

CONCEPTOS BÁSICOS

Para efectos de la interpretación, aplicación y seguimiento del presente Documento de Seguridad para la Protección de Datos Personales del Sindicato Único de Trabajadores al Servicio del Municipio de Atitalaquia, Hidalgo (S.U.T.S.M.A.H.), se establecen los siguientes conceptos básicos, con la finalidad de facilitar la comprensión de las obligaciones, procedimientos y medidas relacionados con el tratamiento y la protección de los datos personales.

1. Datos personales. Cualquier información concerniente a una persona física identificada o identificable, cuya identidad pueda determinarse directa o indirectamente. Puede incluir, entre otros datos, el nombre, domicilio, número telefónico, correo electrónico, CURP, información laboral y datos de identificación.

2. Datos personales sensibles. Aquellos datos personales que afectan la esfera más íntima de su titular o cuya utilización indebida pueden dar origen a discriminación o implicar un riesgo grave. Entre ellos pueden encontrarse los datos relativos a la salud, información genética, origen racial o étnico, creencias religiosas y otros que tengan dicha naturaleza conforme a la legislación aplicable.

3. Titular de los datos personales. La persona física a quien corresponden los datos personales objeto de tratamiento, como pueden ser los agremiados, trabajadores, representantes o cualquier otra persona cuyos datos sean tratados por el Sindicato.

4. Tratamiento de datos personales. Cualquier operación o conjunto de operaciones efectuadas sobre datos personales, mediante procedimientos manuales o automatizados, tales como su obtención, registro, organización, almacenamiento, consulta, utilización, comunicación, transferencia, conservación, bloqueo o supresión.

5. Responsable del tratamiento. La persona física o moral, autoridad u organismo que, conforme al régimen jurídico aplicable, decide sobre el tratamiento de los datos personales,

sus finalidades y los medios utilizados para llevarlo a cabo. La identificación del responsable en el ámbito del Sindicato deberá determinarse de acuerdo con su naturaleza jurídica y las disposiciones aplicables.

6. Encargado del tratamiento. La persona física o moral que realiza el tratamiento de datos personales por cuenta del responsable, conforme a las instrucciones y condiciones que correspondan. Su participación deberá sujetarse a las obligaciones de seguridad y confidencialidad aplicables.

7. Base de datos personales. Conjunto organizado de datos personales referentes a una o varias personas, estructurado de acuerdo con determinados criterios, independientemente del soporte físico o electrónico en el que se encuentre. Puede comprender expedientes impresos, archivos digitales, hojas de cálculo, registros administrativos o sistemas de información.

8. Documento de Seguridad. Instrumento que permite documentar las medidas de seguridad administrativas, físicas y técnicas aplicables a la protección de los datos personales, así como los tratamientos de información, las responsabilidades, los riesgos identificados y las acciones de seguimiento y mejora que correspondan conforme a la normativa aplicable.

9. Medidas de seguridad administrativas. Políticas, procedimientos, controles organizativos y acciones de gestión orientados a proteger los datos personales. Incluyen la asignación de responsabilidades, la capacitación del personal, los compromisos de confidencialidad, la gestión de accesos y la revisión de los procedimientos institucionales.

10. Medidas de seguridad físicas. Acciones y controles destinados a proteger las instalaciones, los archivos, los equipos y los soportes que contienen datos personales frente a daños, pérdida, acceso no autorizado, robo o cualquier otro evento que pueda comprometer su seguridad.

11. Medidas de seguridad técnicas. Controles tecnológicos destinados a proteger los sistemas y la información, como la administración de cuentas de usuario, el uso de contraseñas seguras, los permisos de acceso, las copias de respaldo, las actualizaciones de seguridad y los mecanismos de protección contra accesos no autorizados.

12. Confidencialidad. Condición por la cual los datos personales únicamente pueden ser conocidos o utilizados por las personas autorizadas y para las finalidades que correspondan, evitando su divulgación o acceso indebidos.

13. Integridad. Propiedad que permite preservar la exactitud, consistencia y completitud de los datos personales, evitando modificaciones, alteraciones o destrucciones no autorizadas.

14. Disponibilidad. Condición que permite que los datos personales y los recursos necesarios para su tratamiento puedan ser consultados y utilizados oportunamente por las personas autorizadas cuando se requieran para el desarrollo de sus funciones.

15. Riesgo de seguridad. Posibilidad de que una amenaza aproveche una vulnerabilidad y ocasione consecuencias negativas para los datos personales, las personas titulares o las actividades institucionales.

16. Vulnerabilidad. Debilidad en los procedimientos, instalaciones, equipos, sistemas o controles de seguridad que puede facilitar un acceso no autorizado, la pérdida, alteración o divulgación indebida de datos personales.

17. Amenaza. Circunstancia, evento o acción que puede ocasionar daños a la información personal o comprometer su confidencialidad, integridad o disponibilidad. Puede originarse por errores humanos, fallas técnicas, accesos indebidos, incidentes físicos o actos deliberados.

18. Incidente de seguridad. Evento que compromete o puede comprometer la confidencialidad, integridad o disponibilidad de los datos personales, por ejemplo, la pérdida de expedientes, el envío de información al destinatario equivocado, el acceso no autorizado a archivos o la sustracción de equipos que contienen información personal.

19. Aviso de privacidad. Documento físico, electrónico o presentado en otro formato mediante el cual se informa a la persona titular sobre la existencia y las características del tratamiento de sus datos personales, incluyendo las finalidades correspondientes y los demás elementos exigidos por la legislación aplicable.

20. Consentimiento. Manifestación de la voluntad de la persona titular mediante la cual autoriza el tratamiento de sus datos personales, cuando dicho consentimiento sea exigible conforme a la legislación aplicable y bajo las condiciones establecidas por esta.

21. Derechos de acceso, rectificación, cancelación y oposición (ARCO). Derechos mediante los cuales la persona titular puede solicitar conocer qué datos personales son tratados; pedir la corrección de aquellos que sean inexactos o incompletos; solicitar su cancelación cuando proceda legalmente; u oponerse a su tratamiento en los supuestos previstos por la normativa aplicable.

22. Transferencia de datos personales. Comunicación de datos personales a una persona física o moral, autoridad u organismo distinto de quien los trata, conforme a las condiciones, excepciones y requisitos establecidos en la legislación aplicable.

23. Bloqueo de datos personales. Identificación y conservación de los datos personales una vez cumplida la finalidad para la cual fueron recabados, durante el periodo necesario para atender las responsabilidades que pudieran derivarse de su tratamiento, cuando así corresponda legalmente. Durante esta etapa, su utilización queda limitada a los fines permitidos por la normativa aplicable.

24. Supresión o cancelación de datos personales. Eliminación de los datos personales de los registros, archivos o sistemas correspondientes, cuando proceda conforme a las disposiciones aplicables y se hayan atendido las obligaciones de conservación que correspondan.

25. Inventario de tratamientos de datos personales. Registro organizado que permite identificar los tratamientos efectuados por el Sindicato, las categorías de datos involucradas, sus finalidades, las áreas responsables, los medios de almacenamiento, las personas que intervienen y los plazos de conservación, según corresponda.

26. Plan de trabajo en materia de seguridad. Instrumento de seguimiento que establece las acciones necesarias para atender los riesgos identificados y fortalecer las medidas de seguridad, incluyendo actividades, responsables, prioridades, plazos y mecanismos de verificación.

27. Mejora continua. Proceso de revisión y actualización de las medidas, procedimientos y controles de seguridad, orientado a corregir deficiencias, atender cambios operativos y reducir los riesgos asociados al tratamiento de datos personales.

Los conceptos anteriores tienen como finalidad facilitar la aplicación práctica del presente documento. Su interpretación deberá realizarse de manera congruente con las disposiciones legales vigentes que resulten aplicables al Sindicato. En caso de discrepancia entre una definición operativa y una definición establecida expresamente en la legislación, prevalecerá esta última.

RESPONSABILIDADES

En apego al Art. 78 es responsabilidad del Comité de Transparencia las siguientes funciones:

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 las disposiciones previstas en la presente Ley, la Ley General y en aquellas 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 en aquellas disposiciones aplicables en la materia;

V.- Supervisar en coordinación con las Áreas o unidades administrativas 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 las Autoridades garantes, según corresponda;

VII.- Establecer programas de capacitación y actualización para las personas servidoras públicas en materia de protección de datos personales,

VIII.- Dar vista al órgano interno de control o instancia 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 realicen los responsables.

2. MARCO NORMATIVO

El presente Documento de Seguridad para la Protección de Datos Personales se fundamenta en las disposiciones jurídicas aplicables en materia de protección de datos personales, transparencia, acceso a la información pública y clasificación de la información. Su aplicación deberá atender al régimen jurídico que corresponda al Sindicato Único de Trabajadores al Servicio del Municipio de Atitalaquia, Hidalgo, así como a las obligaciones que, en su caso, le resulten exigibles.

Para la elaboración, aplicación, revisión y actualización de este instrumento, se consideran las siguientes disposiciones:

I. Constitución Política del Estado de Hidalgo.

II. Ley de Transparencia y Acceso a la Información Pública para el Estado de Hidalgo.

III. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Hidalgo.

IV. Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

V. Demás disposiciones jurídicas aplicables.

El Sindicato deberá observar las demás normas, disposiciones y criterios vigentes que resulten aplicables a sus actividades y al tratamiento de datos personales, una vez identificados y validados conforme a su naturaleza jurídica y obligaciones legales.

La aplicación de este marco normativo no deberá interpretarse como una declaración anticipada de que todas las disposiciones citadas son obligatorias para el Sindicato. Su aplicabilidad deberá documentarse y validarse antes de la aprobación definitiva del presente instrumento.

SISTEMA DE GESTIÓN DE DATOS PERSONALES

Es el medio por el cual el Sindicato Único de Trabajadores al Servicio del Municipio de Atitalaquia, Hidalgo, garantiza el tratamiento de los datos personales que lleva a cabo como parte de sus funciones, desde su obtención, uso, registro, conversación, acceso, manejo, aprovechamiento, transferencia, disposición o cualquier otra operación correspondiente; para lo cual, se establecen políticas y métodos orientados a salvaguardar la confidencialidad, integridad y disponibilidad de estos datos, de acuerdo con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Hidalgo y en atención a lo dispuesto en su articulo 53, los elementos queda contenidos en la siguiente tabla y apartados siguientes para quedar como sigue:

CATÁLOGO, DESCRIPCIÓN Y MEDIDAS DE SEGURIDAD DE LOS SISTEMAS DE DATOS PERSONALES DEL SINDICATO ÚNICO DE TRABAJADORES AL SERVICIO DEL MUNICIPIO DE ATITALAQUIA (S.U.T.S.M.A.H.)

II. Nombre, cargo y adscripción.	III. Funciones y Obligaciones.	I.Nombre del Sistema de Tratamiento de Datos Personales	IV. Inventario de datos personales	VII. Tipo de soporte y características donde se resguardan
C. Cleotilde Elizabeth Juárez Cruz Secretaría General	Supervisar el cumplimiento de las medidas de protección en los tratamientos que estén bajo su responsabilidad y autorizar las actuaciones que correspondan conforme a sus atribuciones.	-Expedientes de afiliación -Padrón de agremiados -Actas de sesiones -Expedientes Médicos o Incapacidades	Datos como nombre, domicilio, teléfono particular y/o celular, correo electrónico personal, clave del Registro Federal de Contribuyentes (RFC) Clave Única de Registro de Población (CURP)	Físico; Consiste en documentos y expedientes. Electrónico; Consiste en hojas de cálculo y base de datos relacional.
C. Itaik Onofre Badillo Encargado de Transparencia	Coordinar la integración del Documento de Seguridad, mantener el seguimiento de los pendientes, gestionar las solicitudes de derechos ARCO que correspondan y coordinar las actividades de transparencia relacionadas con datos personales.	-Solicitudes de Transparencia	Datos como nombre, domicilio, teléfono particular y/o celular, correo electrónico personal, clave del Registro Federal de Contribuyentes (RFC) Clave Única de Registro de Población (CURP)	Físico; Consiste en documentos, oficios y expedientes. Electrónico; Consiste en hojas de cálculo y base de datos relacional.
C.Aurea Araceli Montoya Meza Secretaría de Trabajo y Conflictos	Proteger los expedientes de conflictos laborales, quejas y procedimientos que efectivamente gestione, restringiendo el acceso a las	-Quejas y procedimientos laborales.	Datos como nombre, domicilio, teléfono particular y/o celular, correo electrónico personal, clave del Registro Federal de Contribuyentes	Físico; Consiste en documentos, oficios y expedientes. Electrónico; Consiste en hojas de cálculo y base de datos relacional.

	personas autorizadas.		(RFC) Clave Única de Registro de Población (CURP)	
C. Viridiana Facio Corona Secretaría de Finanzas	Resguardar los registros financieros que contengan datos personales y comprobar que su consulta y comunicación se realicen conforme a las atribuciones y finalidades aplicables.	-Cuotas o descuentos sindicales	Datos como nombre, domicilio, teléfono particular y/o celular, correo electrónico personal, clave del Registro Federal de Contribuyentes (RFC) Clave Única de Registro de Población (CURP)	Físico; Consiste en documentos, oficios y expedientes. Electrónico; Consiste en hojas de cálculo y base de datos relacional.
C. Prisciliano Malo Sánchez Secretario de Actas y Acuerdos	Proteger las actas, acuerdos y documentos que incluyan datos personales, verificando su custodia y la elaboración de versiones públicas cuando proceda.	-Actas de sesiones. -Actas de Acuerdos -Actas Informativas.	Datos como nombre, domicilio, teléfono particular y/o celular, correo electrónico personal, clave del Registro Federal de Contribuyentes (RFC) Clave Única de Registro de Población (CURP)	Físico; Consiste en documentos, oficios y expedientes. Electrónico; Consiste en hojas de cálculo y base de datos relacional.
C. Comisión de Honor y Justicia	Resguardar los expedientes que tramite, mantener la confidencialidad de las actuaciones y limitar el acceso según las atribuciones correspondientes.	-Quejas y procedimientos laborales.	Datos como nombre, domicilio, teléfono particular y/o celular, correo electrónico personal, clave del Registro Federal de Contribuyentes (RFC) Clave Única de Registro de Población (CURP)	Físico; Consiste en documentos, oficios y expedientes. Electrónico; Consiste en hojas de cálculo y base de datos relacional.

Fuente: organigrama sindical 2026. La asignación de responsabilidades en materia de datos personales que se propone a continuación es preliminar y no constituye una confirmación de las funciones que actualmente desempeña cada cargo.

CONTROLES Y MECANISMOS DE SEGURIDAD

Objetivo

Establecer las medidas de seguridad que deberán observarse para proteger los datos personales tratados por el Sindicato Único de Trabajadores al Servicio del Municipio de Atitalaquia, Hidalgo, durante su obtención, registro, organización, consulta, utilización, almacenamiento, conservación, comunicación, archivo y, cuando proceda, eliminación.

Las medidas previstas en este apartado buscan preservar la confidencialidad, integridad y disponibilidad de la información, prevenir accesos no autorizados y reducir los riesgos de pérdida, alteración, divulgación o uso indebido.

1. **Medidas de seguridad administrativas:** Conjunto de políticas, procedimientos, acciones y mecanismos de carácter organizacional establecidos por el Sindicato Único de Trabajadores al Servicio del Municipio de Atitalaquia, Hidalgo (S.U.T.S.M.A.H.), destinados a regular, controlar y supervisar el tratamiento de los datos personales bajo su responsabilidad, mediante la asignación de funciones y responsabilidades, la identificación y clasificación de la información, el control de acceso a los expedientes físicos y digitales, la conservación y eliminación segura de documentos, así como la capacitación y sensibilización del personal autorizado, con la finalidad de prevenir el acceso, uso, divulgación, alteración, pérdida o destrucción no autorizada de los datos personales y garantizar su confidencialidad, integridad y disponibilidad, conforme a la normatividad aplicable en materia de protección de datos personales.

2. **Medidas de seguridad físicas:** Buscan proteger los expedientes en papel, los espacios de archivo y los equipos que almacenan o permiten consultar datos personales para prevenir riesgos por caso fortuito o causas de fuerza mayor.

- Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información.
- Prevenir el daño o interferencia a las instalaciones físicas, áreas criticas de la organización, recursos e información.
- Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización; y,
- 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:** Las medidas técnicas comprenden los controles aplicados a las computadoras, cuentas de correo electrónico, plataformas institucionales y demás recursos tecnológicos que se utilicen para tratar datos personales.

- Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;
- Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware; y

- Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

LAS BITÁCORAS DE ACCESO, OPERACIÓN COTIDIANA Y VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES.

Las bitácoras de acceso a los datos personales se utilizan en los soportes físicos y contienen la siguiente información:

- Nombre y cargo de quien accede,
- Identificación del Expediente,
- Fojas del Expediente,
- Propósito del Acceso
- Fecha de Acceso,
- Hora de Acceso,
- Fecha de Devolución
- Hora de Devolución.
- Bitácoras de Vulneración de los Datos Personales
- La bitácora de vulneraciones contiene la siguiente información;
- Nombre de quien reporta el incidente,
- Cargo,
- La fecha en la que ocurrió;
- El motivo de la vulneración de seguridad; y
- Las acciones correctivas implementadas de forma inmediata y definitiva.

ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA

Análisis de riesgos: Debido a las circunstancias generales, tanto físicas como humanas, en las que se tratan datos personales, se ha logrado identificar los siguientes riesgos posibles ante los que se pudiera enfrentar este Sujeto Obligado:

1.- Obtención de datos incompletos o incorrectos.

2.- Omitir la notificación al titular de los datos personales del aviso de privacidad.

No difundir el aviso de privacidad.

No temer evidencia de que el titular de los datos personales conoce los términos del aviso de privacidad, por no tener un consentimiento expreso.

Después de identificar dichos riesgos es necesario hacer un análisis de dichos riesgos, amenazas y sus posibles vulneraciones.

Origen de la amenaza	Causa	Posibles consecuencias
Acceso de personas no autorizadas; sistemas o plataformas oficiales.	Obtención de información o datos personales	Acceso no autorizado, divulgación de datos, robo de información, o modificaciones no autorizadas.

Acceso de criminales o traficantes de datos a los sistemas o plataformas oficiales. (Extorsión)	Adquisición de datos personales para utilizarlos con fines de explotación, chantaje, extorsión o cualquier uso criminal.	Ataques a personas, robo de información, vulneración a la seguridad física y mental de los ciudadanos. Robo de información.
Personal del sujeto obligado con poco conocimiento sobre el tratamiento de datos personales. **Ataques contra otros servidores públicos** **Robo de información.**	Obtención de información para beneficio personal curiosidad, error involuntario o para fines económicos.	Perdida de datos personales, uso indebido, uso ilícito de datos personales, robo de información, extorsión, modificaciones no autorizadas robo de información.
Daño Fisico.	Agua, fuego, accidentes, corrosión.	Daño o pérdida de los datos personales.
Eventos naturales.	Desastres climatológicos, fenómenos meteorológicos, sismos.	Cualquier eventualidad por causa natural, daño o pérdida de los datos personales.
Fallas Técnicas.	Pérdida de electricidad, falla o pérdida de internet, falla en sistemas, correos electrónicos o plataformas oficiales.	Daño o pérdida de los datos personales, divulgación transferencia o modificaciones de datos personales no autorizados.
Decadencias técnicas.	Falta de mantenimiento y/o fallas en equipos.	Poca o absoluta renovación de equipos de telecomunicaciones o cómputos, cambios de voltaje, pérdida, destrucción y daño.
Susceptibilidad en redes o sistemas autorizados.	Falta de contraseñas altamente efectivas, falta de mecanismos para identificar o autentificación de usuarios, falta de actualización de antivirus.	Pérdida, destrucción y daño, divulgación y transferencia de datos personales, modificaciones no autorizadas, robo de información.
Organización.	Procesos carentes de formalidad para administración, acceso, uso y proceso de archivo.	Perdida, destrucción y daño, divulgación y transferencia de datos personales, modificaciones no autorizadas, robo de información.
Espacio donde se archiven.	Carencia de espacio, espacio con poca seguridad, espacio no adecuado, falta de llaves o medidas de seguridad para accesos.	Daño o pérdida de los datos personales, divulgación y transferencia de datos personales, modificaciones no autorizadas robo de información.

Daño y/o alteración de la base de datos que contenga información confidencial.	Carencia de un servidor o sistema que almacene los datos personales, la falta de registros, controles o bitácoras para regular la entrada y salida de personal autorizado, al área donde se almacenan o archivan los datos personales (en su caso los expedientes que los contengan), es un escenario de vulneración y riesgo, facilitando el mal manejo de los datos personales y la pérdida, robo o extravió de expedientes.	Daño y/o perdida de los datos personales. Modificaciones no autorizadas.

"EN PRO DE LA SEGURIDAD SOCIAL"

ANÁLISIS DE BRECHA:

Este constituye un procedimiento de evaluación mediante el cual el Sindicato Único de Trabajadores al Servicio del Municipio de Atitalaquia, Hidalgo, identifica las diferencias existentes entre las medidas de seguridad implementadas para la protección de los datos personales bajo su responsabilidad y aquellas que resultan necesarias para garantizar su adecuado tratamiento, conservación, resguardo y protección.

Este análisis tiene como finalidad identificar posibles vulnerabilidades administrativas, físicas y técnicas que pudieran comprometer la confidencialidad, integridad y disponibilidad de la información personal que se encuentra en posesión del Sindicato, así como establecer las acciones necesarias para prevenir, reducir o corregir los riesgos identificados.

Para su elaboración se consideran las actividades desarrolladas por la Secretaría General, la Comisión de Honor y Justicia y la Unidad de Transparencia, tomando en cuenta los procedimientos mediante los cuales se recaban, utilizan, almacenan, consultan, conservan y, en su caso, eliminan los datos personales.

Derivado de la identificación preliminar de los procesos de tratamiento de información, se establecen los siguientes aspectos sujetos a evaluación:

1. Personal encargado de recabar datos personales;

La recopilación de datos personales corresponde al personal sindical que, de acuerdo con las atribuciones y funciones de cada área, interviene en los procedimientos administrativos, de afiliación, representación sindical, atención de solicitudes, integración de expedientes y demás actividades propias de la organización. El acceso a dicha información deberá limitarse al personal autorizado y exclusivamente para el cumplimiento de las funciones que tenga encomendadas.

2. Espacios físicos destinados a la recopilación de información;

Los datos personales podrán ser recabados dentro de las instalaciones destinadas al funcionamiento del Sindicato, particularmente en los espacios utilizados por la Secretaría General, la Comisión de Honor y Justicia y la Unidad de Transparencia.

En dichos espacios deberán establecerse condiciones que permitan mantener la privacidad durante la recepción de documentos, atención de integrantes del Sindicato y consulta de expedientes, procurando evitar la exposición de información personal ante personas ajenas al procedimiento correspondiente.

3. Medios utilizados para la recopilación de datos personales;

La obtención de información personal podrá realizarse mediante documentos impresos, formatos de afiliación, solicitudes escritas, expedientes administrativos, comunicaciones electrónicas y demás instrumentos relacionados con las actividades sindicales.

Asimismo, se contempla el uso de equipos de cómputo, correo electrónico institucional y medios digitales para la recepción, consulta y almacenamiento de información.

El tratamiento de datos personales mediante estos mecanismos deberá sujetarse a las finalidades institucionales correspondientes y a las medidas de seguridad establecidas en el presente documento.

4. Control de acceso a las áreas de tratamiento de información;

Las instalaciones destinadas al resguardo de documentación sindical deberán contar con mecanismos de control de acceso que permitan restringir la entrada de personas no autorizadas.

Durante la atención de integrantes del Sindicato o de personas que realicen alguna gestión, deberá procurarse que los expedientes, documentos y equipos que contengan datos personales no permanezcan expuestos o disponibles para su consulta por terceros.

Al concluir las actividades laborales, el personal responsable deberá verificar que la documentación utilizada se encuentre debidamente resguardada y que los espacios destinados a su conservación permanezcan bajo condiciones adecuadas de seguridad.

5. Resguardo de documentación física;

Los documentos que contengan datos personales, tales como expedientes de afiliación, padrones de integrantes, registros de cuotas sindicales, documentación relacionada con procedimientos internos, incapacidades médicas y solicitudes de información, deberán conservarse en espacios destinados específicamente para su almacenamiento.

Se deberá procurar que los expedientes se encuentren organizados e identificados conforme a su naturaleza y finalidad, evitando su consulta, reproducción, traslado o disposición por personas que no cuenten con autorización.

Los archiveros, muebles o espacios utilizados para su almacenamiento deberán contar con mecanismos de protección acordes con el nivel de riesgo de la información resguardada.

6. Administración y control de llaves;

Las llaves de acceso a oficinas, archiveros y demás espacios destinados al resguardo de documentos que contengan datos personales deberán permanecer bajo responsabilidad del personal expresamente autorizado.

Su asignación, préstamo, reposición y devolución deberán sujetarse a mecanismos de control que permitan identificar a las personas responsables de su utilización.

Se deberá evitar que las llaves permanezcan al alcance de personas ajenas a las áreas encargadas del tratamiento de la información.

7. Tratamiento y almacenamiento de información digital;

Los datos personales recabados mediante medios electrónicos podrán ser almacenados en los equipos de cómputo utilizados por las áreas sindicales, así como en las cuentas de correo electrónico institucional y dispositivos de almacenamiento autorizados.

El personal que intervenga en su tratamiento deberá utilizar mecanismos de autenticación y protección que permitan reducir el riesgo de accesos no autorizados, pérdida, alteración, divulgación o eliminación indebida de la información.

Asimismo, deberán establecerse criterios para regular el uso de memorias USB, discos duros portátiles y otros medios de almacenamiento externo, considerando los riesgos asociados a su traslado, conexión y conservación.

8. Uso del correo electrónico institucional;

El correo electrónico utilizado por el Sindicato constituye un medio de comunicación y recepción de documentación que puede contener datos personales.

En consecuencia, deberán establecerse mecanismos para controlar su acceso, administrar las credenciales de autenticación y determinar las responsabilidades del personal que tenga autorización para utilizarlo.

Cuando una cuenta de correo sea utilizada por más de una persona autorizada, deberán implementarse controles que permitan delimitar responsabilidades, reducir los riesgos derivados del uso compartido y garantizar la protección de la información recibida o enviada.

9. Integración de expedientes y conservación documental;

Una vez recabados los datos personales, el área responsable procederá, cuando corresponda, a integrar el expediente físico o electrónico respectivo, de conformidad con la naturaleza del procedimiento administrativo o sindical.

La documentación deberá organizarse de manera que permita su identificación, localización y consulta por el personal autorizado, evitando la duplicación innecesaria de información.

Los expedientes deberán conservarse durante los plazos que resulten aplicables conforme a las disposiciones legales, administrativas y archivísticas correspondientes.

10. Consulta y utilización de datos personales;

Durante el desarrollo de las actividades sindicales, los datos personales únicamente deberán consultarse y utilizarse para las finalidades legítimas que motivaron su recopilación, así como para aquellas que resulten legalmente procedentes.

El personal responsable deberá evitar la reproducción, transmisión, divulgación o utilización de información para fines ajenos a las atribuciones y actividades institucionales.

Toda consulta deberá observar los principios de confidencialidad, responsabilidad y seguridad establecidos en la normativa aplicable.

11. Conclusión de procedimientos y resguardo de expedientes;

Al concluir un procedimiento de afiliación, gestión administrativa, atención de solicitudes, intervención de la Comisión de Honor y Justicia o cualquier otro trámite que implique el tratamiento de datos personales, la documentación generada deberá integrarse y resguardarse conforme a los criterios institucionales de organización documental.

La conclusión de un procedimiento no implica la eliminación automática de los datos personales, por lo que deberán observarse los plazos de conservación aplicables y, una vez cumplidos, los procedimientos autorizados para su disposición documental.

12. Copias de seguridad y recuperación de información;

Con la finalidad de prevenir la pérdida accidental, deterioro o eliminación indebida de información digital, deberán establecerse procedimientos para la generación, conservación y recuperación de copias de seguridad de los archivos electrónicos que contengan datos personales.

Dichos procedimientos deberán definir la periodicidad de los respaldos, los medios autorizados para su almacenamiento, el personal responsable de su ejecución y los mecanismos para verificar la posibilidad de recuperar la información.

La implementación de estas medidas deberá realizarse de manera gradual y documentada, conforme a los recursos disponibles y al nivel de riesgo identificado.

13. Identificación de vulnerabilidades y medidas correctivas;

Como parte del análisis de brecha, deberán evaluarse las posibles vulnerabilidades relacionadas con el acceso a las instalaciones, resguardo de expedientes físicos, utilización de equipos de cómputo, administración de contraseñas, empleo de dispositivos externos, almacenamiento electrónico y conservación de documentos.

Los riesgos identificados deberán registrarse y valorarse considerando su probabilidad de ocurrencia y el impacto que pudieran ocasionar sobre los derechos de las personas titulares de los datos personales.

A partir de dicha evaluación se establecerán medidas preventivas y correctivas, identificando a las áreas responsables de su implementación, los recursos necesarios y los plazos correspondientes.

14. Medidas de seguridad para transferencias: las transferencias al interior del sujeto obligado y a otros sujetos obligados:

1) Solo podrán ser transferidos los datos personales para dar seguimiento y conclusión al trámite o sistema de tratamiento previsto.

2) El área que entrega los datos personales deberá cerciorarse de transferir la totalidad de los datos que resulten necesarios para el seguimiento o la conclusión del trámite o sistema correspondiente limitando la entrega de información que no sea requerida o necesaria.
3) Se deberá corroborar que la información entregada sea completa y veraz.

4) El área o dependencia que reciba los datos personales deberá conservar los mismos sujetándose a los lineamientos y finalidad del aviso de privacidad de este sujeto obligado y adoptando las medidas de seguridad previstas en este documento.

5) El área que reciba los datos personales deberá encargarse de la supresión de los datos que reciba cuando esta corresponda.

6) El área que entrega y el área que recibe los datos personales deberán dar acceso a los datos personales tratándose de procedimientos de derecho ARCO.

7) Notificar mediante oficio, a la Unidad de Transparencia, la transferencia de datos personales, la finalidad, el medio y la unidad administrativa o dependencia a quienes fueron transferidos.

   Medidas de seguridad en caso de vulneraciones: en caso de ocurrir laguna deberán registrarse en la bitácora de vulneraciones, aclarando la fecha en la que ocurrió y las acciones correctivas implementadas de forma inmediata y definitiva.

Seguimiento y mejora continua;

Las medidas de seguridad administrativas, físicas y técnicas establecidas en el presente Documento de Seguridad deberán someterse a procesos de revisión y actualización, particularmente cuando se identifiquen nuevas amenazas, modificaciones en los procedimientos institucionales, incorporación de herramientas tecnológicas o incidentes que puedan comprometer la protección de datos personales.

El Sindicato, por conducto de las áreas responsables, deberá promover la aplicación de controles proporcionales a los riesgos identificados, procurando fortalecer progresivamente los mecanismos de protección de la información.

En consecuencia, el análisis de brecha constituye un instrumento de evaluación y mejora continua que permitirá orientar las acciones institucionales hacia la reducción de vulnerabilidades, el fortalecimiento de las medidas de seguridad y el cumplimiento de las obligaciones legales en materia de protección de datos personales.

Monitoreo y revisión

Se propone establecer revisiones periódicas con evidencia documental, incluyendo:

- Cambios en sistemas, responsables o finalidades.
- Altas y bajas de usuarios autorizados.
- Resultados de respaldos y pruebas de recuperación.
- Incidentes reportados y medidas correctivas.
- Cumplimiento de capacitación.
- Avance del plan de trabajo.
- Cambios normativos que afecten las obligaciones institucionales.

La actualización también deberá realizarse cuando ocurran cambios sustanciales en el tratamiento, se detecten nuevas amenazas o se implementen medidas correctivas derivadas de una vulneración.

CONCLUSIONES.

El presente Documento de Seguridad para la Protección de Datos Personales del Sindicato Único de Trabajadores al Servicio del Municipio de Atitalaquia, Hidalgo, constituye un instrumento institucional orientado a establecer las directrices, responsabilidades, procedimientos y medidas de seguridad administrativas, físicas y técnicas necesarias para procurar la protección de los datos personales que se encuentran bajo su tratamiento y resguardo, en el ejercicio de sus funciones y atribuciones.

Su elaboración responde al compromiso institucional de promover una cultura de protección de datos personales, fortalecer los mecanismos de control interno y establecer criterios que permitan prevenir, identificar, atender y reducir los riesgos asociados al acceso no autorizado, pérdida, alteración, destrucción, divulgación o uso indebido de la información personal.

Asimismo, el presente documento se concibe como un instrumento de aplicación permanente, evaluación y mejora continua, cuya implementación y actualización deberán realizarse de manera progresiva, atendiendo a las necesidades operativas del Sindicato, los resultados de las evaluaciones de seguridad y las disposiciones jurídicas que resulten aplicables.

En este sentido, el Documento de Seguridad deberá ser revisado y, en su caso, actualizado cuando se presenten las siguientes circunstancias:

I. Cuando se produzcan modificaciones sustanciales en los procedimientos, sistemas, medios de almacenamiento o actividades relacionadas con el tratamiento de datos personales que impliquen cambios en los niveles de riesgo previamente identificados.

II. Cuando, como resultado de los procesos de supervisión, monitoreo, evaluación y mejora continua, se identifique la necesidad de fortalecer, modificar o incorporar medidas de seguridad administrativas, físicas o técnicas.

III. Cuando se detecten vulnerabilidades, amenazas o incidentes de seguridad que puedan comprometer la confidencialidad, integridad o disponibilidad de los datos personales bajo resguardo del Sindicato.

IV. Cuando resulte necesario implementar acciones correctivas o preventivas derivadas de una vulneración de seguridad, con la finalidad de mitigar sus consecuencias y reducir la posibilidad de que se presenten situaciones similares.

V. Cuando se realicen modificaciones en la estructura organizacional del Sindicato, en las funciones de las áreas responsables o en las atribuciones del personal que interviene en el tratamiento y resguardo de datos personales.

VI. Cuando se emitan reformas legislativas, disposiciones normativas, criterios, lineamientos o requerimientos por parte de las autoridades competentes que resulten aplicables a las actividades de tratamiento de datos personales realizadas por el Sindicato.

VII. Cuando, derivado de observaciones, recomendaciones o propuestas formuladas por las personas integrantes del Sindicato, sus órganos de representación o las personas responsables del manejo de la información, se identifiquen oportunidades para fortalecer los procedimientos y mecanismos de protección de datos personales.

Finalmente, el Sindicato Único de Trabajadores al Servicio del Municipio de Atitalaquia, Hidalgo, reconoce la importancia de establecer mecanismos de protección de la información personal como parte fundamental de una gestión institucional responsable, transparente y respetuosa de los derechos de las personas.

Por lo anterior, el presente Documento de Seguridad establece las bases para la implementación, seguimiento y fortalecimiento progresivo de las medidas de protección de datos personales, promoviendo la participación y corresponsabilidad de quienes intervienen en su tratamiento, así como la observancia de los principios de confidencialidad, integridad, disponibilidad y seguridad de la información, de conformidad con el marco jurídico que resulte aplicable por tanto no es producto acabado, es perfectible, sujeto a constante revisión y por tanto actualización y mejora.

Transparencia del Sindicato Único de Trabajadores
al Servicio del Municipio de Atitalaquia Hidalgo
(S.U.T.S.M.A.H) Ubicado en las Oficinas del Sindicato, Fray Diego de Rodríguez S/N, Col. Centro aun costado del Auditorio Municipal.

T.P.S.E. Cleotilde Elizabeth Juárez Cruz.
Secretaria General del Sindicato Único de Trabajadores al Servicio del Municipio de Atitalaquia Hidalgo.

Encargado de Transparencia; Arq. Itaik Onofre Badillo
Correo Electrónico: atitalaquiasindicato@gmail.com