DOCUMENTO DE SEGURIDAD

H. AYUNTAMIENTO DE METEPEC, HIDALGO

2024-2027

INDICE

INTRODUCCIÓN

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados en el artículo 29, establece los principios y bases para tener una correcta protección de datos personales para ser empleados en el municipio de Metepec Hidalgo.

El documento de seguridad nos ayuda a proteger los datos personales, así como cualquier información resguardada en el sujeto obligado.

No toda persona tiene permitido conocer los datos personales, se debe proteger la confidencialidad e integridad de cada individuo, es por ello surgen los documentos de seguridad que cuenta con inventario de datos, roles y deberes, análisis de riesgo y un plan de trabajo con el fin de cuidar los datos personales que nos definen como persona.

Para un buen tratamiento de los datos personales, se deben adoptar medidas necesarias como acciones, la escritura del documento, desglosar la información bien, anexos para una buena comprensión siendo responsable, transparente y lícito en el marco normativo.

A continuación, se presenta como se tratan los datos personales, así como su resguardo en el municipio de Metepec Hidalgo para una mejor comprensión;

NORMATIVIDAD APLICABLE

Con este documento de seguridad, se da cumplimiento a lo establecido de manera general, al Artículo 29 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. De manera particular, el responsable deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente:

I. El inventario de datos personales y de los sistemas de tratamiento;
II. Las funciones y obligaciones de las personas que traten datos personales;
III. El análisis de riesgos;
IV. El análisis de brecha;
V. El plan de trabajo;
VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y
VII. El programa general de capacitación.

De igual manera, se da cumplimiento a lo referido en el Artículo 30 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados en donde se establece las razones por las cuales se deben de actualizar el documento de seguridad y son las siguientes;

I. Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;
II. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;
III. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida, y
IV. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

En caso de que ocurra una vulneración a la seguridad, el responsable deberá analizar las causas por las cuales se presentó e implementar en su plan de

trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales si fuese el caso a efecto de evitar que la vulneración se repita.

PRINCIPIOS Y DEBERES

El Artículo 3 fracción XI de La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados, reconoce cuatro Derechos a los Particulares: Acceso, Rectificación, Cancelación y Oposición (ARCO). De igual forma, el Artículo 10 de la misma ley, establece obligaciones a los sujetos obligados que a continuación se enlistan:

PRINCIPIOS;

1. Licitud
2. Finalidad
3. Lealtad
4. Consentimiento
5. Calidad
6. Proporcionalidad
7. Información
8. Responsabilidad

DEBERES;

1. Confidencialidad
2. Seguridad

GLOSARIO DE TÉRMINOS

Para efectos del presente documento se entenderá por:

Áreas: Instancias de los sujetos obligados previstas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes, que

cuentan o puedan contar, dar tratamiento, y ser responsables o encargadas de los datos personales;

Autoridades garantes: Órgano de control y disciplina del Poder Judicial; los órganos internos de control de los órganos constitucionales autónomos; las contralorías internas del Congreso de la Unión; el Instituto Nacional Electoral, por cuanto hace al acceso a la protección de datos personales a cargo de los partidos políticos; y los órganos encargados de la contraloría interna u homólogos de los Poderes Ejecutivo, Legislativo y Judicial, así como de los órganos constitucionales autónomos, de las Entidades Federativas;

Aviso de privacidad: Documento a disposición de la persona titular de la información de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de estos;

Comité de Transparencia: Instancia a la que hace referencia el artículo 39 de la Ley General de Transparencia y Acceso a la Información Pública;

Consentimiento: Manifestación de la voluntad libre, específica e informada de la persona titular de los datos mediante la cual se efectúa el tratamiento de estos;

Datos personales: Cualquier información concerniente a una persona identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información;

Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para ésta. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o

futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;

Derechos ARCO: Derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales;

Documento de seguridad: Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales;

Plataforma Nacional: Plataforma Nacional de Transparencia a que hace referencia el artículo 44 de la Ley General de Transparencia y Acceso a la Información Pública;

Sujetos Obligados: Cualquier autoridad, entidad, órgano y organismo de los poderes ejecutivo, legislativo y judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, en el ámbito federal, estatal y municipal o de las demarcaciones territoriales de la Ciudad de México;

Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales, y

Unidad de Transparencia: Instancia a la que hace referencia el artículo 41 de la Ley General de Transparencia y Acceso a la Información Pública.

TIPOS PRINCIPALES DE SEGURIDAD:

- **Seguridad física:** Protege los bienes tangibles, edificios, instalaciones y personas mediante control de accesos, cercas, cámaras de vigilancia y guardias.
- **Ciberseguridad:** Resguarda los sistemas informáticos, redes, programas y dispositivos conectados frente a ataques digitales y robos de datos en línea.
- **Seguridad de la información:** Cuida los datos confidenciales y documentos de una entidad, sin importar si están en formato digital o físico.
- **Seguridad operacional:** Define las reglas, procesos y acciones cotidianas para evitar riesgos y proteger los recursos sensibles durante el trabajo diario.

I. INVENTARIO Y CATÁLOGO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO

El Inventario de Tratamientos de Datos Personales es el control documentado que se lleva a cabo de los tratamientos de datos personales que realizan las áreas.

Los elementos que actualmente se identifican en el Inventario de cada uno de los tratamientos son los siguientes:

- Nombre de la unidad administrativa.
- Nombre del tratamiento.
- Finalidad.
- Fundamento normativo.
- Datos personales que se recaban.
- Forma de obtención de los datos personales.

- Cargos de las personas que tienen acceso a la base de datos.
- Tipo de soporte en el que se almacena la base de datos personales.
- Referencia documental conforme al Catálogo de Disposición Documental vigente.
- Información sobre transferencias de datos personales.
- Plazo de conservación.

Los **Avisos simplificados e integrales** fueron elaborados para que se colocaran en las instalaciones de cada una de las áreas responsables que así lo requirieran, en tanto se recaban datos de manera presencial; mientras que los integrales se ubicaron en el repositorio de avisos de privacidad integrales del Portal de Datos Personales.

Los Avisos se pueden consultar en el repositorio: https://metepechidalgo.gob.mx/index.php/transparencia/avisos-de-privacidad. Cabe señalar que los Avisos se actualizan constantemente por parte de las áreas u órganos, en tanto se modifican los tratamientos de datos personales o se registran nuevos que lo requieren.

En cumplimiento a lo establecido en los artículos 36, 37 y 38 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Hidalgo, ponemos a su disposición los Avisos de Privacidad que cada Unidad Administrativa expresa, vigila y cumple en el ejercicio de sus funciones, trámites y servicios, todo de acuerdo con lo establecido en la normativa vigente correspondiente.

II. LAS FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATEN DATOS PERSONALES

Las funciones y obligaciones incluyen garantizar el cumplimiento de la ley, emitir y difundir avisos de privacidad, e implementar medidas de seguridad administrativas, técnicas y físicas. También deben capacitar al personal, designar un área o persona responsable del tratamiento y proteger los datos contra daños, pérdidas o accesos no autorizados.

- **Garantizar el cumplimiento de la ley**: Asegurar que el tratamiento de datos cumpla con los principios y obligaciones establecidos en la legislación aplicable.
- **Emitir y dar a conocer el aviso de privacidad**: Informar a los titulares de los datos, antes de recopilar la información, sobre el tratamiento al que serán sometidos sus datos.
- **Establecer medidas de seguridad**: Implementar y mantener medidas administrativas, técnicas y físicas para proteger los datos personales contra daños, pérdida, alteración, destrucción o acceso no autorizado.
- **Proteger la confidencialidad, integridad y disponibilidad:** Asegurar que los datos estén protegidos contra accesos no autorizados, manipulación o pérdida.
- **Capacitar al personal**: Diseñar e impartir capacitación a los empleados sobre la protección de datos, de acuerdo con sus roles y responsabilidades.
- **Permitir el ejercicio de derechos ARCO:** Implementar herramientas para que los titulares puedan ejercer sus derechos de acceso, rectificación, cancelación y oposición.

III. EL ANÁLISIS DE RIESGOS

Para la confección del primer Documento de Seguridad y ante la necesidad de determinar las medidas de seguridad que debían adoptar las áreas responsables, resultaba necesario conocer el nivel de riesgo que representaba cada tratamiento de datos personales. Para ello, fue necesario calcular los factores de riesgo por tipo de dato, por tipo de acceso y por entorno desde el cual se realizan los tratamientos de los datos personales.
En el cálculo del nivel de riesgo de cada uno de los tratamientos registrados se usó como referencia la Metodología de Análisis de Riesgo BAA, la cual se conoce así por las tres variables en las que se enfoca para determinar el nivel de riesgo de los datos personales:

1. Beneficio para el atacante.
2. Accesibilidad para el atacante.
3. Anonimidad del atacante.

El análisis de riesgo tiene como objetivo principal ordenar la protección de los datos personales que se traten en el Municipio de Metepec, Hidalgo, con la evolución de las actividades que se realizan en el mismo, que son cada vez con mayor, pues para anticiparse y prepararse para los nuevos retos que se suscitan día con día, lo recomendable es tener una responsabilidad proactiva ante el tratamiento de los datos personales gestionando los riesgos y el impacto que estos podrían generar.

En ese sentido, la gestión de riesgos, consiste en implementar un conjunto de acciones definidas con el propósito de controlar la probabilidad de consecuencias o impactos que una actividad puede tener sobre los datos personales que posee el Municipio de Metepec Hidalgo, los cuales han de ser protegidos, pues se pretende garantizar el servicio público que se otorga, por lo que debe de identificarse la naturaleza, ámbito y fines de los tratamientos de datos personales, para poder detectar los niveles de posible vulnerabilidad de la información.

IV. EL ANÁLISIS DE BRECHA

El análisis de brecha permite identificar la distancia que existe entre las medidas recomendadas y las medidas implementadas por cada uno de los tratamientos reportados.

Se ha analizado los servicios que se llevan a cabo en el H. Ayuntamiento, para brindar un mejor servicio y atención a los tramites que se realizan dentro del municipio de Metepec hidalgo. Se ha comparado la agilidad de los tramites a consideración de la administración anterior y han incrementado de manera favorable.

V. PLAN DE TRABAJO

El documento de seguridad busca enmarcar los deberes de las Áreas Administrativas de las dependencias, para la máxima protección de datos personales. Debido a la importancia y el contexto actual en materia de datos personales, se debe mantener actualizado el plan de trabajo, el cual permita alcanzar los objetivos del sistema de seguridad de protección de datos personales.

La finalidad de este plan de trabajo es plasmar las actividades que las Áreas Administrativas de las dependencias, realizarán para la aplicación del presente documento de seguridad. Lo anterior se realizará con base a las atribuciones establecidas en Ley de Protección de Datos Personales en Posesión de sujetos Obligados.

1. Se avisará al director o encargado responsable de cada área sobre el documento de seguridad para ser aplicable.
2. Seguir en continua capacitación para reafirmar la protección de datos personales de los servidores públicos a ciudadanía.
3. Contar con la documentación necesaria para cumplir con el principio de transparencia.
4. Mantener actualizados toda documentación que proteja los datos personales en posesión de sujetos obligados.

VI. LOS MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

La Dependencia de la Administración de Metepec Hidalgo, deberá implementar como mínimo las siguientes medidas generales de seguridad, para evitar daños, extraer información no autorizada generada y administrada dentro del sujeto obligado:

1. Asignar un espacio seguro y adecuado para el tratamiento de datos personales, que no se encuentre a la vista del público y que

preferentemente no sea un área de paso frecuente por el personal del trabajo o ajeno al mismo.

2. Tener bajo llave o asegurados los archiveros, archivos, cajas y almacenes en donde se encuentre almacenada la información de datos personales.
3. Evitar que se dejen descuidados o sin la atención debida documentos que contengan datos personales.
4. Establecer un plan de contingencia con protocolos de seguridad, designación de responsables, procedimientos de control, señalizaciones y medidas de protección física contra incendio, explosión, humedad, plaga y cualquier otra forma de desastre natural o humano.
5. Verificar que en ningún caso los documentos que contengan datos personales se utilicen como papel reciclable ni de doble uso, ya que una vez transcurridos los plazos en que deban cancelarse o al tratarse de proyectos no utilizables, deberán ser destruidos.
6. Implementar programas de capacitación en materia de protección de datos personales al interior del Municipio de Metepec Hidalgo.

Con estas acciones, se podrán identificar las mejoras que habrán de implementarse para el adecuado manejo y protección de los datos personales.

VII. EL PROGRAMA GENERAL DE CAPACITACIÓN

El programa de capacitaciones en materia de Protección de Datos Personales se llevará a cabo de manera anual, cuyo objetivo es concientizar a los servidores públicos del municipio de Metepec Hidalgo, a la materia de protección de datos personales, para tener una mayor comprensión de la responsabilidad que conlleva el trabajar con información personal de ciudadanos y trabajadores del Municipio, así como informar sobre las medidas de seguridad básicas que se deben de llevar a cabo para proteger la información que contiene datos personales.

FUNCIONES PRINCIPALES

- **Proteger datos:** Cuidar la información personal de accesos o robos no autorizados.
- **Definir reglas:** Establecer qué debe hacer el personal y cómo debe usar los equipos o sistemas.
- **Prevenir riesgos:** Encontrar fallas o peligros antes de que dañen los sistemas.
- **Cumplir la ley:** Demostrar ante las autoridades que se siguen las normas de protección de datos.

El presente documento de seguridad se actualizará siguiendo las bases descritas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.