

PACHUCA
CAPITAL DE LA TRANSFORMACIÓN
2024 ✦ 2027

GACETA
MUNICIPAL

EDICIÓN
81



30 DE SEPTIEMBRE DE 2026

DIRECTORIO

C. JORGE ALBERTO REYES HERNÁNDEZ
PRESIDENTE MUNICIPAL CONSTITUCIONAL

C. ARELY SÁNCHEZ OLIVARES
SÍNDICA PROCURADORA HACENDARIA

C. JENNY MARLÚ MELGAREJO CHINO
SÍNDICA PROCURADORA JURÍDICA

C. EDUARDO TREJO LINO
SECRETARIO GENERAL

REGIDORES

C. FRANCISCO DE JESÚS PÉREZ BALLESTEROS

C. SHARON MICHELL ARROYO DIAZ

C. MANUEL CANALES PÉREZ

C. ELIZABETH REGNIER CANO

C. ARLAN CRUZ OLVERA

C. NORA HILDA SALAS ACUÑA

C. CLAUDIO ERICK MERCADO PÉREZ

C. CARMELA ZAMORA PÉREZ

C. JUAN DE DIOS ROSAS MENESES

C. ANA LAURA PÉREZ GODÍNEZ

C. IVONNE BERENICE ESPITIA GARNICA

C. MARÍA LUISA OVIEDO QUEZADA

C. NADIA REYNA CAMACHO

C. FERNANDA GUERRERO ACEVEDO

C. CARLOS GARCÍA MONZALVO

C. ÁNGEL CASTAÑEDA MALDONA

C. KARLA STHEPANIE MOTA ULAJE

C. HUMBERTO AUGUSTO VERAS GODOY

C. MANELICH ENRIQUE MONDRAGÓN ARMIJO

EDITORIAL

C. JUAN RAMÓN SOBERANES IBARRA
OFICIAL MAYOR DEL H. AYUNTAMIENTO

C. JORGE ALBERTO HERNÁNDEZ GÓMEZ
DIRECTOR DE COMUNICACIÓN SOCIAL

CONTENIDO

**Manual de tratamientos y Medidas de Seguridad
para la Protección de Datos Personales, del
Municipio de Pachuca de Soto.**

Manual de Tratamientos y Medidas de Seguridad para la Protección de Datos Personales, del Municipio de Pachuca de Soto.

Versión 1.0

Tratamientos y Medidas de Seguridad.

Introducción.

El derecho a la protección de datos personales, es un derecho fundamental reconocido internacionalmente, es un derecho de carácter subjetivo, autónomo y de tercera generación, el manejo de datos personales no debe verse de forma aislada ya que forma parte de un sistema donde se encuentran conectados varios componentes: la transparencia, el derecho de acceso a la información, y la protección de datos personales, mismos que se entrelazan en torno al núcleo de la libertad de expresión.

La finalidad de este manual tiene como propósito proteger los datos personales en posesión del Municipio de Pachuca de Soto, como sujeto obligado, para regular su tratamiento legítimo controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas obligadas. Así como también, fijar los mecanismos y procedimientos que nos permitan dar cumplimiento a las Obligaciones de Seguridad y Confidencialidad de los datos personales, mediante el establecimiento de una estrategia para determinar las acciones concretas a seguir por parte de las dependencias y entidades de la Administración Pública Municipal como áreas responsables de la información, respecto del tratamiento y manejo de los datos personales cuyas finalidades son necesarias, de conformidad a los principios establecidos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Lo anterior, deriva a que actualmente la sociedad se encuentra en un cambio permanente en el que se ven involucradas las nuevas tecnologías de la información, el uso constante de internet y redes sociales, lo cual ha causado preocupación y mayor interés en el manejo de datos personales ya que implica una responsabilidad tanto para el que otorga la información, como del que la recibe. Por ello, la información que fluye en dichas interacciones debe preservar el derecho de la persona a la privacidad y a la protección de sus datos, considerándose necesaria la elaboración del presente manual, con la finalidad de que el personal del Municipio de Pachuca de Soto se familiarice y sensibilice con la seguridad de la información y la protección de los datos personales, para implementar medidas de seguridad efectivas que contribuyan a mitigar las posibles vulneraciones a la información clasificada como confidencia y a la seguridad de los datos personales en posesión de este sujeto obligado.



Tratamientos y Medidas de Seguridad.

Objetivo.

Establecer las bases mínimas y condiciones homogéneas para el personal de las diferentes unidades administrativas municipales que por sus funciones y competencias traten datos personales, garantizando el cumplimiento de las obligaciones en materia de seguridad y confidencialidad de datos personales que se encuentran bajo su responsabilidad, a efecto de protegerlos de manera sistemática y continua.

Marco Normativo.

1. La Constitución Política de los Estados Unidos Mexicanos en materia de derecho de acceso a la información y protección de datos personales en posesión de sujetos obligados;
2. La Ley General de Transparencia y Acceso a la Información Pública LGTAIP (D.O.F. 20/03/2025);
3. La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, LGPDPPSO (D.O.F. 20/03/2025);
4. La Constitución Política del Estado de Hidalgo;
5. Ley de Transparencia y Acceso a la Información Pública del Estado de Hidalgo; y
6. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Hidalgo, LPDPPSOEH.

Alcance.

Dirigido a los todos los servidores públicos, que por sus funciones y competencias conozcan y apliquen las medidas de seguridad mínimas para el tratamiento de datos personales, en las diferentes unidades administrativas que conforman el Municipio de Pachuca de Soto.



1. Conceptos Generales.

Definición de Dato Personal.

La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Hidalgo, la define como cualquier información concerniente a una persona física identificada o identificable. De manera general, una persona física puede entenderse como todo miembro de la especie humana con la posibilidad de adquirir derechos y contraer obligaciones, su información como individuo se encuentra protegida por dicha ley. De manera específica se considera a la persona física como el titular a quien corresponden los datos personales.

En lo que respecta a las empresas, organizaciones, asociaciones, etc. (conocidas en el ámbito jurídico como “personas morales”), su información corporativa y comercial por regla general no es considerada como datos personales sujeta a la protección de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados; sin embargo, tal información se protege por otros ordenamientos legales.

Tipo de Datos Personales.

Según su naturaleza y régimen de protección, los datos personales se pueden clasificar en tres:

I. Datos personales en General: 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;

II. 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;

III. Datos Biométricos: Son los datos personales relacionados con las características físicas, fisiológicas o de comportamiento de una persona física, que permite o confirma la identificación única de la misma.



Tratamientos y Medidas de Seguridad.

Datos Personales		
Generales	Sensibles	Biométricos
Nombre, domicilio, teléfono de contacto, correo electrónico personal, actividades, experiencia laboral y profesional, etc.	Origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas filosóficas y morales, afiliación sindical, opiniones políticas,	Huella dactilar, el reconocimiento facial, vascular, de iris o retina; y la geometría de la mano u oreja.

Elaboración propia con información obtenida en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Hidalgo.

Principios de la Protección de Datos Personales.

Todo tratamiento de datos personales que efectúe el personal responsable de las dependencias y entidades de la Administración Pública Municipal en su día a día, tienen como obligación el proteger la información personal a la que tienen acceso, de conformidad a los siguientes principios:

1. **Licitud.** - A través de este principio se obliga al responsable a que el tratamiento de los datos personales que recabe, lo realice con apego y cumplimiento a las disposiciones legales aplicables. Al respecto, es obligación de los servidores públicos responsables de asistir a las capacitaciones y/o pláticas que se impartan al respecto.
2. **Finalidad.** - De conformidad con este principio, los datos personales solamente podrán ser recabados y tratados para cumplir con las finalidades establecidas en el aviso de privacidad correspondiente. Por lo anterior, para poder llevar a cabo el tratamiento de los datos personales para cualquier otra finalidad que no se encuentre establecida en el aviso de privacidad se deberá obtener el consentimiento de los titulares y el aviso de privacidad deberá ser modificado para informar sobre las nuevas finalidades. Al respecto los servidores públicos que como parte de sus funciones traten datos personales, deben conocer cuáles son las finalidades que dieron origen al tratamiento de datos personales y que las mismas son necesarias para la relación jurídica entre el municipio y el titular, así como aquéllas que no lo son.



Tratamientos y Medidas de Seguridad.

3. **Lealtad.** - Todos los datos personales deberán tratarse privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad por lo que, bajo ningún supuesto, se deberán recabar datos personales a través de medios engañosos o fraudulentos. En lo que se refiere a la expectativa razonable de privacidad, ésta se entiende como la confianza que deposita cualquier persona en otra, con respecto a que los datos personales proporcionados entre ellos serán tratados conforme a lo que acordaron.
4. **Consentimiento.** - De conformidad con este principio, se establece que el responsable deberá obtener el consentimiento para el tratamiento de los datos personales salvo ciertas excepciones de ley. Se debe obtener el consentimiento previo del titular de los datos para poder realizar el tratamiento de su información. Por regla general el consentimiento tácito es suficiente. Éste se obtiene cuando habiendo puesto a disposición de los titulares el aviso de privacidad, no se manifieste su oposición, salvo que una Ley exija que la voluntad del titular se manifieste de manera expresa, en tal caso el responsable deberá ser capaz de demostrar de manera indubitable que el titular otorgó su consentimiento, ya sea a través de una declaración o una acción afirmativa clara, es decir por escrito, a través de firma autógrafa, firma electrónica o cualquier otro mecanismo de autenticación que al efecto se establezca. No es necesario el consentimiento para el tratamiento de los datos personales:
 - I. Cuando una norma con rango de Ley señale expresamente que no será necesario el consentimiento del titular para el tratamiento de sus datos personales, por razones de seguridad pública, salud pública, disposiciones de orden público o protección de derechos de terceros;
 - II. Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;
 - III. Para el reconocimiento o defensa de derechos del titular ante autoridad competente;
 - IV. Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;
 - V. Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;



Tratamientos y Medidas de Seguridad.

- VI. Cuando los datos personales sean necesarios para la prevención, el diagnóstico médico, la prestación de servicios de asistencia sanitaria, el tratamiento médico, o la gestión de servicios sanitarios;
 - VII. Cuando los datos personales figuren en fuentes de acceso público;
 - VIII. Cuando los datos personales se sometan a un procedimiento previo de disociación; y
 - IX. Cuando el titular sea una persona reportada como desaparecida en los términos de la Ley en la materia.
5. **Calidad.** - Para cumplir con el principio de calidad, es obligación tratar los datos personales exactos, completos, pertinentes, correctos y actualizados atendiendo a las finalidades para las cuales fueron recabados. Cuando los datos son proporcionados por los titulares, se entiende que el responsable se encuentra en cumplimiento de este principio.
6. **Proporcionalidad.** - De conformidad con el principio de proporcionalidad, los servidores públicos responsables, deberán llevar a cabo el tratamiento solamente de aquellos datos personales que resulten necesarios, adecuados y relevantes en relación para las finalidades para las que se hayan obtenido. Conforme a este principio, se debe seguir un criterio de minimización, en términos del cual los datos personales que se traten sean los mínimos necesarios de acuerdo con las finalidades para los que se requieran.
7. **Información.** - El responsable deberá dar a conocer al titular, a través del aviso de privacidad, la información relativa a la existencia y características principales del tratamiento a que serán sometidos sus datos personales.
8. **Responsabilidad.** – Los servidores públicos responsables, deberán velar y responder por el tratamiento de los datos personales que mantiene bajo su posesión, y también por aquellos que hubiere comunicado a un tercero.

Derecho de los Titulares de Datos Personales.

1.- Derecho ARCO.

En cualquier momento, el titular o su representante podrán solicitar al Municipio de Pachuca como responsable de su información, el acceso, rectificación, cancelación u oposición respecto del tratamiento de los datos personales que le conciernen.



Tratamientos y Medidas de Seguridad.

A	Acceso	El titular tendrá derecho de acceder a sus datos personales que obren en posesión del responsable, así como a conocer la información relacionada con las condiciones, generalidades y particularidades de su tratamiento
R	Rectificación	El titular tendrá derecho a solicitar al responsable la rectificación o corrección de sus datos personales, cuando éstos resulten ser inexactos, incompletos o no se encuentren actualizados.
C	Cancelación	El titular tendrá derecho a solicitar la cancelación de sus datos personales de los archivos, registros, expedientes y sistemas del responsable, a fin de que los mismos ya no estén en su posesión.
O	Oposición	El titular podrá oponerse al tratamiento de sus datos personales o exigir que se cese en el mismo, respecto de aquellas finalidades que resulten aplicables.

Elaboración propia con información obtenida en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Hidalgo.

2.- Derecho de Portabilidad.

Cuando se traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado, el titular tendrá derecho a obtener del responsable una copia de los datos personales objeto de tratamiento, en un formato electrónico estructurado y comúnmente utilizado, el cual le permita seguir utilizándolos, conforme a los plazos, términos y requerimientos establecidos.

Cuando el titular haya facilitado los datos personales y el tratamiento se base en el consentimiento o en un contrato o relación jurídica, tendrá derecho a transferir dichos datos personales y cualquier otra información que haya facilitado y que se conserve en un sistema de tratamiento automatizado a otro sistema, en un formato electrónico comúnmente utilizado, sin impedimentos por parte del responsable de quien se retiren los datos personales. En otras palabras, te permite llevar tus datos de una plataforma a otra de forma sencilla y controlada.

El Municipio como Sujeto Responsable.

Se entenderá como responsable el que obtiene los datos personales directamente del titular, cuando éste los proporciona personalmente o por algún medio que permita su entrega directa al responsable como son, de manera enunciativa más no limitativa, medios electrónicos, ópticos, sonoros, visuales, vía telefónica, Internet o cualquier otra tecnología o medio.



Tratamientos y Medidas de Seguridad.

El Municipio como sujeto responsable deberá adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos y según se requiera para el cumplimiento de las finalidades concretas, explícitas lícitas y legítimas que motivaron su tratamiento. Se presume que se cumple con la calidad en los datos personales, cuando éstos son proporcionados directamente por el titular y hasta que éste no manifieste y acredite lo contrario.

Además, deberá implementar los mecanismos necesarios para acreditar el cumplimiento de los principios, deberes y obligaciones establecidas en la Ley de la materia, así como para rendir cuentas al titular y a la Autoridad Garantes sobre los tratamientos de datos personales que efectúe, para lo cual podrá valerse de estándares, mejores prácticas nacionales o internacionales o de cualquier otro mecanismo que determine adecuado para tales fines. Lo anterior, aplicará aun cuando los datos personales sean tratados por parte de un encargado, así como al momento de realizar transferencias de datos personales.

Quien maneja los Datos Personales.

Para acceder a los datos personales obtenidos o recabados es importante identificar los roles de quienes intervienen en su tratamiento:

Roles	Descripción
Titular	Persona física a quien corresponde los datos personales.
Responsable	Corresponde a las personas servidoras públicas de la dependencia y entidades de la Administración Pública Municipal que llevan a cabo el tratamiento de datos personales.

Elaboración propia, con información obtenida de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Hidalgo.

Consentimiento para el Tratamiento de Datos Personales.

Las Unidades Administrativas Municipales como responsables de los tratamientos, deberán obtener el consentimiento del titular para el manejo de sus datos personales, de manera previa, cuando los recabe directamente de éste. Cuando se recabe datos personales indirectamente del titular y se requiera de su consentimiento conforme a las disposiciones Legales, éste no podrá tratar los datos personales hasta que cuente con la manifestación de la voluntad libre, específica e



Tratamientos y Medidas de Seguridad.

informada del titular, mediante la cual autoriza el tratamiento de los mismos, ya sea tácita o expresa según corresponda.

Consentimiento	Descripción
Tácito	Cuando habiéndose puesto a disposición del titular el aviso de privacidad, éste no manifieste su voluntad en sentido contrario.
Expreso	Cuando la voluntad del titular se manifieste de forma verbal, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología.

Elaboración propia con información obtenida en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Hidalgo.

Para la obtención del consentimiento de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad declarada por Ley, se estará a lo dispuesto en las reglas de representación previstas en la legislación civil que resulte aplicable en el Estado de Hidalgo.

El responsable deberá obtener el consentimiento expreso y por escrito del titular para el tratamiento de datos personales sensibles, salvo que se actualice alguna de las causales de excepción previstas en la Ley, se considerará que el consentimiento expreso se otorgó por escrito cuando el titular lo externe mediante un documento con su firma autógrafa, huella dactilar o cualquier otro mecanismo autorizado por la normativa aplicable.

En el entorno digital, podrán utilizarse medios como la firma electrónica o cualquier mecanismo o procedimiento equivalente que permita identificar fehacientemente al titular, y a su vez, recabar su consentimiento de tal manera que se acredite la obtención del mismo.

Transferencias y Remisiones de Datos Personales.

De conformidad a la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados para el Estado de Hidalgo, se considera como transferencia a toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado, misma que se encuentra sujeta al consentimiento expreso de su titular, salvo las excepciones previstas por la Ley, y deberá ser informada al titular en el aviso de privacidad, así como limitarse a las finalidades que las justifiquen.



Tratamientos y Medidas de Seguridad.

El responsable podrá realizar transferencias de datos personales sin necesidad de requerir el consentimiento del titular en los siguientes supuestos:

- I. Cuando la transferencia esté prevista en Ley o Tratados Internacionales suscritos y ratificados por México.
- II. Cuando la transferencia se realice entre responsables, siempre y cuando los datos personales se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;
- III. Cuando la transferencia sea legalmente exigida para la investigación y persecución de los delitos, así como la procuración o administración de justicia;
- IV. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho ante autoridad competente, siempre y cuando medie el requerimiento de esta última;
- V. Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, el tratamiento médico o la gestión de servicios sanitarios, siempre y cuando dichos fines sean acreditados;
- VI. Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular; y
- VII. Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero.

Toda transferencia deberá formalizarse mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, de conformidad con la normatividad que le resulte aplicable al responsable.

Las **remisiones** de datos personales tienen lugar cuando el Municipio comparte con una persona física o moral ajena a este nacional o internacional, a fin de que dicho tercero preste un servicio al responsable de los datos y que pueda cumplir con el objeto de la relación con el titular de los mismos. Las remisiones nacionales e internacionales de datos personales que se realicen entre responsable y encargado no requerirán ser informadas al titular, ni contar con su consentimiento.

Aviso de Privacidad.

Las dependencias y entidades de la Administración Pública Municipal tienen dentro de sus principales obligaciones, como responsables del tratamiento de datos personales, el de contar con un aviso de privacidad, el cual, de conformidad con la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Hidalgo, es el documento físico, electrónico o en cualquier otro formato generado por el responsable, que es puesto a disposición del titular con el objeto de informarle los propósitos principales del tratamiento al que serán sometidos sus datos personales. El no contar con el aviso de privacidad, o bien, omitir en el mismo



Tratamientos y Medidas de Seguridad.

alguno de los elementos previstos en la Ley según sea el caso, serán sancionadas por la autoridad correspondiente.

Es importante señalar que todo responsable de datos personales debe, por regla general, poner a la vista o podrán entregar de manera física a los titulares de datos personales un aviso de privacidad previo a recabar sus datos personales. Todos los particulares que tratan datos personales, deben cumplir con el principio de información y esto se logra principalmente con la puesta a disposición de los titulares del aviso de privacidad.

Propósito del Aviso de Privacidad.

El aviso de privacidad tiene como propósito principal informar a los titulares sobre el alcance, términos y condiciones generales del tratamiento, a fin que sus datos personales y sobre los derechos con los que cuentan en relación con el tratamiento de su información personal, el titular pueda decidir si desea entregarle sus datos al responsable y, en su caso, saber con qué derechos cuenta en relación con sus datos personales. En otras palabras, el aviso de privacidad proporciona a los particulares información para tomar decisiones informadas en relación a sus datos personales y saber que cuentan con cierto control y con la facultad de disponer de su información y deberá caracterizarse por ser sencillo, con información necesaria, expresado en lenguaje claro y comprensible, y con una estructura y diseño que facilite su entendimiento y se pondrá a disposición del titular en dos modalidades, el simplificado y el integral.

Elementos a Considerar en el Aviso de Privacidad.

El aviso de privacidad tendrá por objeto informar al titular sobre los alcances y condiciones generales del tratamiento, a fin de que esté en posibilidad de tomar decisiones informadas sobre el uso de sus datos personales y, en consecuencia, mantener el control y disposición sobre ellos.

El **aviso simplificado** deberá contener la siguiente información:

- I. La denominación del responsable;
- II. Las finalidades del tratamiento;
- III. Cuando se realicen transferencias de datos personales que requieran consentimiento;



Tratamientos y Medidas de Seguridad.

- IV. Los mecanismos y medios disponibles para que el titular, en su caso, pueda manifestar su negativa para el tratamiento de sus datos personales para finalidades y transferencias de datos personales que requieren el consentimiento del titular; y
- V. El sitio donde se podrá consultar el aviso de privacidad integral.

El **aviso integral** deberá contener la siguiente información:

- I. El domicilio del responsable;
- II. Los datos personales que serán sometidos a tratamiento;
- III. El fundamento legal que faculta expresamente al responsable para llevar a cabo el tratamiento y las transferencias de datos personales que efectúen;
- IV. Los medios y procedimientos disponibles para ejercer los derechos ARCO;
- V. El domicilio de la Unidad de Transparencia; y
- VI. Los medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad.

Tipos de Aviso de Privacidad.

Para la difusión del aviso de privacidad, que garantice y cumpla con el principio de información, podrá valerse de los formatos siguientes:

-
- **Físicos:** medio impreso en papel;
 - **Electrónicos:** utilización de medios digitales: página oficial, sitio web y correo electrónico;
 - **Medios verbales:** sonoro, vía telefónica, o
 - **Cualquier otra tecnología.**
-

Elaboración propia, con información obtenida a través de los Lineamientos Generales de Protección de Datos Personales para el Sector Público y páginas de internet.



2. Protección a los Datos Personales.

Importancia de los Datos Personales y su Protección.

El Municipio como sujeto obligado conoce y da cuenta de manera general sobre las medidas de seguridad de carácter Administrativo, físico y técnico adoptadas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee; por las siguientes razones:

- La protección de datos personales es un derecho humano de los titulares que se encuentra reconocido en la Constitución Política de los Estados Unidos Mexicanos, en los tratados internacionales y en la normatividad aplicable y, a su vez, es una obligación para quienes los tratan.
- Para ayudar a prevenir y mitigar los riesgos de vulneración a la seguridad de los datos personales.
- Para mejorar los procesos en el manejo de datos personales de las Unidades Administrativas que integran el municipio, así como el nivel de confianza de los titulares de los datos personales.

También será aplicable las medidas de seguridad 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, que se efectúe en las dependencias y entidades de la Administración Pública Municipal que conforman el Municipio, como responsables de su manejo, que permitan garantizar la protección, confidencialidad, disponibilidad e integridad de los datos personales.

Principales Obligaciones para la Protección de Datos Personales.

El responsable de la información de cada dependencia y entidades de la Administración Pública Municipal, deberá obtener el consentimiento del titular para el tratamiento de sus datos personales, de manera previa, cuando los recabe, éste no podrá tratar los datos personales hasta que cuente con la manifestación de la voluntad libre, específica e informada del titular, mediante la cual autoriza el tratamiento de los mismos, ya sea tácita o expresa según corresponda.

El responsable deberá adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de



Tratamientos y Medidas de Seguridad.

que no se altere la veracidad de éstos y según se requiera para el cumplimiento de las finalidades concretas, explícitas lícitas y legítimas que motivaron su tratamiento, además deberá suprimir los datos personales en su posesión cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades concretas, explícitas, lícitas y legítimas que motivaron su tratamiento, previo bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos; en la supresión de los datos personales, el responsable deberá implementar métodos y técnicas orientadas a la eliminación definitiva de éstos.

Los plazos de conservación de los datos personales, no deberán exceder de aquéllos que sean necesarios para el cumplimiento de las finalidades concretas, explícitas lícitas y legítimas que justificaron su tratamiento.

En el establecimiento de los plazos de conservación de los datos personales, el responsable deberá considerar los valores administrativos, contables, fiscales, jurídicos e históricos de los datos personales, así como atender las disposiciones aplicables en la materia de que se trate.

Además el responsable procurará que las personas con algún tipo de discapacidad o pertenecientes a un grupo vulnerable, puedan ejercer, en igualdad de circunstancias, su derecho a la protección de datos personales, para lo cual deberá promover acuerdos con instituciones públicas especializadas que pudieran auxiliarle en la recepción, trámite y entrega de las respuestas a solicitudes para el ejercicio de los derechos ARCO en lengua indígena, braille o cualquier formato accesible correspondiente, en forma más eficiente.

Ciclo de Vida de los Datos Personales.

Para establecer y mantener las medidas de seguridad para la protección de los datos personales, las dependencias y entidades de la Administración Pública Municipal deberán observar el presente manual para la gestión y tratamiento de los datos personales, para que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su **obtención, almacenamiento, uso y posterior supresión.**



Tratamientos y Medidas de Seguridad.

Etapa I. Obtención.

Esta etapa se considera como la inicial del ciclo de vida y se asocia con el acto de crear, adquirir o incorporar información nueva que no existía con anterioridad en el área.

Etapa II. Almacenamiento y Uso

1. **Almacenamiento:** es el proceso de envío de la información recién capturada al almacenamiento persistente (discos duros, discos ópticos, memorias USB, archivos físicos, entre otros). bajo principio de finalidad y calidad.
2. **Uso:** en esta fase la información recabada (transformada), se aplica en la ejecución de las tareas del área bajo los principios de calidad, información y finalidad, o que es transferida a otro sujeto obligado.

Etapa III. Supresión

1. **Archivo:** corresponde al resguardo de la información documental o digital que haya cumplido con lo señalado en el Catálogo de Disposición Documental.
2. **Destino final:** Con base en el Catálogo de Disposición Documental, se debe identificar si la información -que contiene el dato personal- se suprime o se conserva como indefinida.

Elaboración propia, con información obtenida a través de los Lineamientos Generales de Protección de Datos Personales para el Sector Público y de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Hidalgo.

Etapas del Ciclo de Vida de Datos Personales.

I.- Obtención.

Conforme a las funciones y obligaciones del personal responsable de las dependencias y entidades de la Administración Pública Municipal involucrado en el tratamiento de datos personales del municipio; deberán contar con el inventario de los datos personales y de las bases y/o sistemas de sus tratamientos, la obtención de los datos personales podrá obtenerse de manera directa o indirectamente del titular, independientemente de los formatos o medios físicos y/o electrónicos utilizados para tal fin, en función de las finalidades para las cuales fueron recabados, de conformidad a sus tratamientos.



Tratamientos y Medidas de Seguridad.

Inventario de Datos Personales del Municipio de Pachuca de Soto.

Derivado de los principios de legalidad, proporcionalidad y finalidad, la Unidad de Transparencia del Municipio de Pachuca, requirió información a los responsables de las diferentes dependencias y entidades de la Administración Pública Municipal, para identificar qué tipo de datos personales manejan para el cumplimiento de sus atribuciones, en cuyo ejercicio se conoció que de acuerdo a sus tratamientos se identificaron un total de 83 datos personales, de acuerdo a la información básica de sus tratamientos, mismo que se integra de la siguiente manera:

No.	Datos Personales
1	Acta constitutiva
2	Acta de defunción
3	Acta de matrimonio
4	Acta de nacimiento
5	Antecedentes tóxicos/adicciones
6	Área de adscripción del puesto
7	Beneficiarios
8	Calidad migratoria
9	Características Físicas (rasgos fisonómicos o media filiación de una persona)
10	Carta de exposición de motivos
11	Carta poder
12	Cartilla militar
13	Cédula profesional
14	Certificado de estudios académicos
15	Certificado medico
16	Clave Única de Registro de Población (CURP)
17	Código postal
18	Comprobante de ingresos
19	Comprobante de domicilio
20	Comprobante de egresos
21	Comprobante de estudios
22	Constancia de antecedentes no penales
23	Constancia de no inhabilitación laboral
24	Constancia de situación fiscal
25	Contrato de arrendamiento
26	Correo electrónico institucional
27	Correo electrónico particular
28	Credencia para votar (INE)



Tratamientos y Medidas de Seguridad.

29	Cuentas Bancaria, número de cuenta bancaria y/o Clave Bancaria Estandarizada (CLABE)
30	Curriculum vitae
31	Datos familiares (cónyuge, hijos, padres, hermanos)
32	Datos personales emocionales/psicológicos
33	Domicilio
34	Edad
35	Estado civil
36	Estatura
37	Estudio Socioeconómico
38	Expediente laboral
39	Fecha de nacimiento
40	Firma autógrafa
41	Firma electrónica
42	Fotografía de adultos
43	Fotografías de niños y niñas
44	Huella dactilar/digital
45	Identidad facial
46	Información bancaria de los particulares
47	Información generada durante los procedimientos de reclutamiento, selección y contratación
48	Información relacionada con el expediente clínico, y en general, toda aquella relacionada con el estado de salud
49	Información relacionada con el patrimonio de una persona física
50	Licencia de conducir
51	Licencia de construcción
52	Licencia de funcionamiento
53	Licencia de uso de suelo
54	Licencia oficial de portación de armas
55	Lugar de nacimiento (origen)
56	Lugar de residencia
57	Nacionalidad
58	Nombre (adulto)
59	Nombre (menor de edad)
60	Nombre del servidor público
61	Número de empleado
62	Número de Seguridad Social
63	Número telefónico
64	Ocupación
65	Opinión de cumplimiento SAT
66	Origen étnico
67	Padrón de proveedores



Tratamientos y Medidas de Seguridad.

68	Peso de una persona
69	Posturas religiosas/ideológicas/morales/filosófica
70	Orientación sexual
71	Profesión u ocupación
72	Puesto desempeñado
73	Reacciones alérgicas
74	Referencias laborales
75	Régimen de sociedad conyugal
76	Registro Federal de Contribuyentes (RFC)
77	Salario o sueldo
78	Sexo/genero
79	Talla de una persona
80	Tipo de discapacidad
81	Tipo de sangre
82	Tipo y modalidad de la violencia
83	Usuarios y contraseñas de sistemas

Elaboración propia, con información obtenida a través del oficio número PMP/SCyT/0174/2025.

Precisando que los datos personales obtenidos son los adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento, de conformidad a las atribuciones conferidas por los diversos ordenamientos legales establecidos para cada una de las dependencias y entidades de la Administración Pública Municipal.

II.- Almacenamiento y Uso.

Cada dependencia y entidades de la Administración Pública Municipal deberá almacenar los datos personales para preservar la información y que esté disponible para su uso cuando se requiera, procesarla, organizarla y estructurarla a fin de facilitar su localización, deberá estar plenamente identificado y almacenado en uno o más lugares físicos y/o electrónicos de cada soporte documental de acuerdo a los fines de cada tratamiento.



Tratamientos y Medidas de Seguridad.

Sitios de Resguardo	Medios de Almacenamiento	Ubicación
Oficina de la Institución	Físicos	Cajones de escritorio
		estantes / archiveros
	Digital	Computadoras escritorio
		Computadoras Laptop
		Teléfonos inteligentes, tables y otros dispositivos móviles.
		Memoria USB, discos duros extraíbles, y otros medios de almacenamiento digital
		Almacenamiento en líneas/computo en la nube.

Elaboración propia, con información obtenida a través de los Lineamientos Generales de Protección de Datos Personales para el Sector Público y a la consulta en páginas de internet.

III.- Supresión.

Corresponde a la baja archivística de los datos personales conforme a las disposiciones jurídicas aplicables en materia de archivos, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable, de cada dependencia y entidades de la Administración Pública Municipal quien deberá establecer y documentar los procedimientos para su conservación.

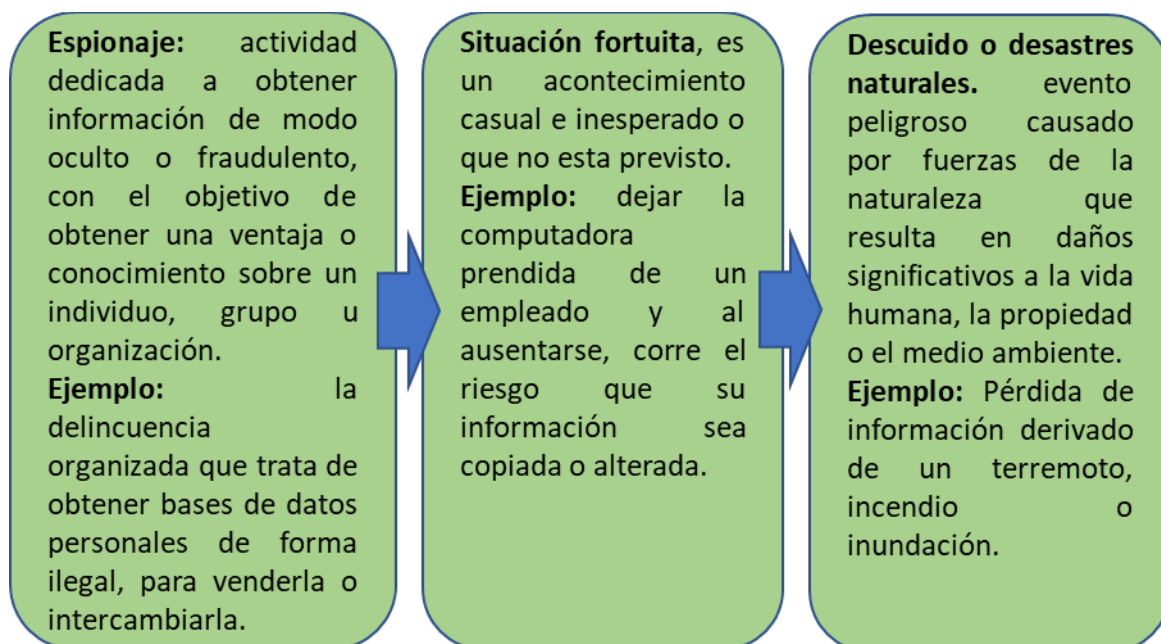


3. Medidas de Seguridad.

Propósito de las Medidas de Seguridad.

Las dependencias y entidades de la Administración Pública Municipal deberán implementar y operar las medidas de Seguridad para proteger los datos personales en posesión de los servidores públicos responsables, esto para regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la libertad informativa. Así como fijar mecanismos, procedimientos y términos, para reducir el riesgo al que están expuestos los datos personales durante su ciclo de vida, ya que esto podría provocar un daño a los derechos de las personas, al no proteger los intereses de la persona titular y la expectativa razonable de privacidad.

Las medidas de seguridad también ayudan a que, en caso de presentarse un incidente, se reduzca el daño en las dependencias y entidades de la Administración Pública Municipal, razón por la cual es importante identificar los distintos orígenes que tienen los riesgos a los que están expuestos los datos personales, por ejemplo:

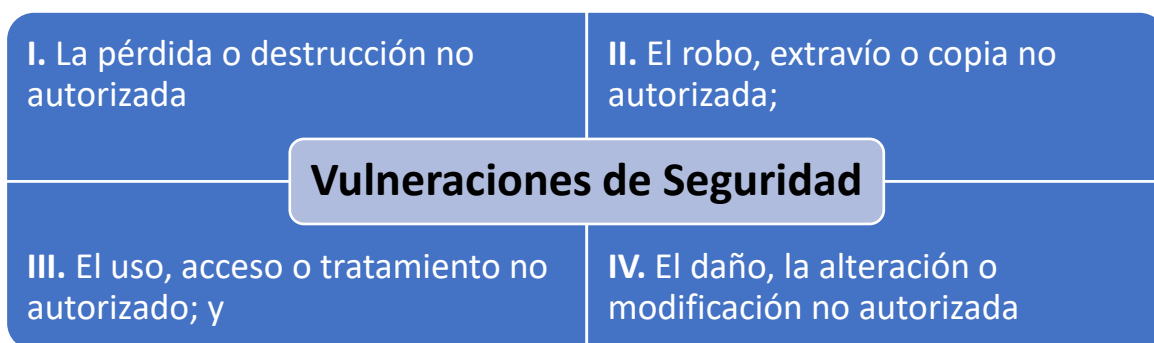


Elaboración propia con información obtenida en página de internet.



Tratamientos y Medidas de Seguridad.

Además, las dependencias y entidades de la Administración Pública Municipal deberán monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, para que en su caso se diseñe y apliquen diferentes niveles de capacitación de su personal, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales; así como también actualizar su contenido cuando ocurran los siguientes eventos:



Elaboración propia con información obtenida en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Hidalgo.

Los responsables deberán llevar una bitácora de las vulneraciones de seguridad en caso de que estas ocurran e informar al titular y a la autoridad garante, a fin de que los titulares afectados puedan tomar las medidas correspondientes, además deberán analizar las causas por las cuales se presentó para implementar un plan de trabajo con las acciones preventivas y correctivas para su contención, y evitar que la vulneración se repita.

Con independencia del lugar físico y el tipo de sistema electrónico en el que se encuentren los datos personales que manejen las dependencias y entidades de la Administración Pública Municipal, o el tipo de tratamiento que se efectúen, el responsable deberá establecer y mantener las medidas de seguridad necesarias de carácter **administrativo, físico y técnico** para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración o destrucción, así como su uso, acceso o tratamiento no autorizado, garantizando su confidencialidad, integridad y disponibilidad.



Tratamientos y Medidas de Seguridad.

Medidas de Seguridad	
Tipo	Descripción
Administrativas	Refiere a las políticas y procedimientos para la gestión, soporte y revisión de la seguridad de los datos personales a nivel organizacional, la identificación, clasificación y borrado seguro de los datos personales, así como la sensibilización y capacitación del personal en materia de protección de datos personales.
Físicas	Corresponde al conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.
Técnicas	Al conjunto de acciones y mecanismos que se valen de la tecnología relacionada con equipos y sistemas informáticos para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento.

Elaboración propia con información obtenida en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Hidalgo.

Análisis de Riesgo.

Como principal causa por las que ocurre el robo o extravío de datos personales, o información relevante para las instituciones, es simplemente porque los datos no se protegen adecuadamente, por lo que se establecen las siguientes acciones de control de cada una de las dependencias y entidades de la Administración Pública Municipal, derivado de los riesgos de la siguiente manera:

a). Medidas de Seguridad Administrativas.

Corresponde a la políticas y procedimientos establecidos para garantizar la seguridad de los datos personales dentro de las dependencias y entidades de la Administración Pública Municipal.

Descripción	Acción de Control
No dejar a la vista información personal.	Políticas de escritorio limpio: no dejar a la vista documentos importantes, llaves de escritorio, y bloquear el equipo de cómputo cuando no se ocupe. Hábitos de cierre y resguardo: que cada empleado cierre sus cajones, y que las cosas importantes siempre se mantengan bajo llave si no están en uso.



Tratamientos y Medidas de Seguridad.

	• Impresoras, escáneres, copiadoras y buzones limpios: no dejar abandonados documentos en áreas de uso común.
• Establecer Mecanismos para eliminar de manera segura la información.	• Destrucción segura de documentos: Los documentos y otros medios físicos se deben destruir antes de ser desechados, por ejemplo, con triturado. • Borrar o eliminar la información en equipo de cómputo y medios de almacenamiento digital: utilizar herramientas de software que borran de “forma segura” archivos digitales específicos o dispositivos de almacenamiento completos. • Fijar periodos de resguardo y destrucción de información: identificar de manera periódica la información que ya cumplió con su fin y que puede ser almacenada en el archivo de concentración o que puede ser destruida o eliminada de conformidad a los procedimientos establecidos de baja o destrucción. • Tomar precauciones en el uso de documentos reciclados: al utilizar bandejas de papel reciclado, no reutilizar documentos con datos personales.
• Documentar las responsabilidades en la protección de datos personales.	• Informar al personal sobre la importancia de la seguridad y protección de datos: comunicar al personal involucrado en el tratamiento de datos personales de manera explícita que tiene una responsabilidad sobre la información en su custodia. • Fomentar la cultura de la seguridad de la información: difundir, la importancia de establecer el uso de medidas de seguridad y buenos hábitos de tratamiento de los datos. • Difundir noticias en temas de seguridad: difundir las medidas de seguridad implementadas en la Institución. • Asegurar la protección de datos personales en contrataciones: mediante el establecimiento de cláusulas que especifiquen claramente el tratamiento y las medidas de seguridad implementadas para la protección de los datos personales.



Tratamientos y Medidas de Seguridad.

Medidas de Seguridad Físicas.

Corresponden a las acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.

Descripción	Acción de Control
Establecer las medidas de seguridad en las áreas de trabajo.	• Resguardar el área de trabajo: no permitir que alguien sin motivos relacionados al funcionamiento del área ingrese al entorno de trabajo. • Establecer bitácoras de registro para el personal ajeno al área de trabajo: establecer un registro de acceso al personal ajeno que ingresa y sale del área de trabajo. • Establecer bitácoras, para usuarios: uso de bitácoras, donde se anote la fecha, hora, nombre de la persona que accede a un expediente para su consulta.
• Establecer medidas de seguridad para evitar robos.	• Establecer Cerraduras y candados: en las gavetas, escritorios, o archiveros se puedan cerrar con llave. • Elementos preventivos disuasorios: implementar medidas de seguridad preventivos como alarmas, guardias de seguridad, rejas, maletines de seguridad, entre otros.
• Establecer medidas de seguridad para el movimiento de información entre áreas de trabajo.	• Aprobación de salida de equipo de cómputo y/o medios de almacenamiento digital: establecer pases de salida y entrada de los equipos mencionados. • Traslado de documentos: para la entrega de documentos de datos personales, deberán ser entregados de manera personal por el propio personal del área remitente. • Usar mensajería certificada: para el caso de envío de información de datos personales de documentos o expedientes que contengan datos personales y por cuestiones de distancia requieran ser enviados por un tercero, se realice por medio de mensajería certificada.



Tratamientos y Medidas de Seguridad.

Medidas de Seguridad Técnicas

Corresponde a las medidas de seguridad aplicables en toda la infraestructura tecnológica, control de acceso, operación de las comunicaciones e infraestructura y sistemas de información.

Descripción	Acción de Control
Actualización a los equipos de Cómputo.	Actualización del sistema operativo: los equipos de cómputo tendrán que contar con el sistema operativo actualizado de acuerdo con sus características técnicas. Actualización del software: el software que se utilice debe ser adecuado a las actividades de cada área y con las actualizaciones necesarias para su correcto funcionamiento. Actualización del hardware: considerar las actividades de cada área para la asignación de equipos de cómputo, que estos cuenten con las características técnicas adecuadas a las necesidades de los usuarios.
Actualización del software instalado en los equipos de Cómputo.	Uso de software actualizado: la actualización periódica evita posibles vulnerabilidades externas. Restricción de uso de software distinto al Institucional: evitar utilizar software de dudosa procedencia ya que puede contener virus o programas de ataque y acceso a ciberdelinquentes a la información institucional. Mantenimiento Preventivo: revisión y escaneo de los equipos de cómputo, con el fin de descartar infecciones por algún software malicioso.
Medidas de Seguridad para el acceso al entorno de trabajo digital.	Uso de contraseñas y/o cifrado: toda información institucional en un medio digital deberá estar protegida por contraseña y/o cifrado, para así evitar el acceso no autorizado y/o posibles eventos de robo o pérdida de información. Bloqueo y cierre de sesiones: cuando no se utilice el equipo de cómputo se debe bloquear o cerrar la sesión de usuario.



Tratamientos y Medidas de Seguridad.

	• Gestión de usuarios y accesos: en caso de usar más de una persona el mismo acceso para los sistemas institucionales, con el mismo usuario y contraseña, se debe suprimir esta mala práctica.
• Establecer medidas de seguridad para navegar en entornos digitales.	• Reglas de navegación segura: sólo se deben navegar en sitios web básicos para el desempeño de sus funciones, evitando aquellos sitios no relacionados de riesgo o que violen los derechos de autor. • Reglas para la divulgación de información: antes de enviar información a un tercero, almacenarla en la nube, publicarla en un sitio web, o compartirla en redes sociales, se debe evaluar si esta acción no está poniendo en riesgo a titulares o a personal de la Institución. • Uso de conexiones seguras: además de verificar que los protocolos de navegación sean seguros, se debe cuidar que la conexión también sea confiable.

Análisis de Brecha.

Después de haber realizado un análisis a los riesgo determinados para la protección de datos personales, y considerando las amenazas y vulnerabilidades existentes, además de los recursos involucrados para su tratamiento, a continuación se presenta el análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes, a fin de determinar el plan de trabajo para la implementación de las medidas de seguridad faltantes, de conformidad con los tratamiento de los datos personales.

No.	Medida de Control	Existente		Observación
		Si	No	
I.- Medidas de Seguridad Administrativas				
I.1	No dejar a la vista información personal.			
I.1.1	Políticas de escritorio limpio	X		Implementadas de manera parcial
I.1.2	Hábitos de cierre y resguardo		X	
I.1.3	Impresoras, escáneres, copiadoras y buzones limpios	X		
I.2	Establecer Mecanismos para eliminar de manera segura la información			
I.2.1	Destrucción segura de documentos		X	Implementadas de manera parcial
I.2.2	Borrar o eliminar la información en equipo de cómputo y medios de almacenamiento digital	X		
I.2.3	Fijar periodos de resguardo y destrucción de información	X		
I.2.4	Tomar precauciones en el uso de documentos reciclados		X	



Tratamientos y Medidas de Seguridad.

I.3	Documentar las responsabilidades en la protección de datos personales			
I.3.1	Informar al personal sobre la importancia de la seguridad y protección de datos	X		Implementadas de manera parcial
I.3.2	Fomentar la cultura de la seguridad de la información		X	
I.3.3	Difundir noticias en temas de seguridad		X	
I.3.4	Asegurar la protección de datos personales en contrataciones		X	
II.- Medidas de Seguridad Físicas				
II.1	Establecer las medidas de seguridad en las áreas de trabajo			
II.1.1	Resguardar el área de trabajo	X		Implementadas de manera parcial
II.1.2	Establecer bitácoras de registro para el personal ajeno al área de trabajo		X	
II.1.3	Establecer bitácoras, para usuarios		X	
II.2	Establecer medidas de seguridad para evitar robos.			
II.2.1	Establecer Cerraduras y candados	X		Implementadas de manera parcial
II.2.2	Elementos preventivos disuasorios	X		
II.3	Establecer medidas de seguridad para el movimiento de información entre áreas de trabajo.			
II.3.1	Aprobación de salida de equipo de cómputo y/o medios de almacenamiento digital		X	Implementadas de manera parcial
II.3.2	Traslado de documentos	X		
II.3.3	Usar mensajería certificada		X	
III.- Medidas de Seguridad Técnicas				
III.1	Actualización a los equipos de Cómputo.			
III.1.1	Actualización del sistema operativo.	X		Implementadas de manera parcial
III.1.2	Actualización del software	X		
III.1.3	Actualización del hardware		X	
III.2	Actualización del software instalado en los equipos de Cómputo.			
III.2.1	Uso de software actualizado		X	Por implementar
III.2.2	Restricción de uso de software distinto al Institucional		X	
III.2.3	Mantenimiento Preventivo		X	
III.3	Medidas de Seguridad para el acceso al entorno de trabajo digital.			
III.3.1	Uso de contraseñas y/o cifrado		X	Implementadas de manera parcial
III.3.2	Bloqueo y cierre de sesiones		X	
III.3.3	Gestión de usuarios y accesos	X		
III.4	Establecer medidas de seguridad para navegar en entornos digitales			
III.4.1	Reglas de navegación segura		X	Por implementar
III.4.2	Reglas para la divulgación de información		X	
III.4.3	Uso de conexiones seguras		X	

Elaboración propia con información de las acciones de control determinadas por el Municipio de Pachuca de Soto.

De lo anterior, como resultado del análisis de brecha realizado a las acciones de control determinadas como medidas de seguridad para la protección de datos personales, a continuación, se presenta el plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de la gestión de los tratamientos realizados por cada una de las



Tratamientos y Medidas de Seguridad.

dependencias y entidades de la Administración Pública Municipal como responsables de los datos personales, mismas que se clasifican de acuerdo al tipo de acción que se implementara:

- Acciones de control de carácter documental-administrativo,
- Acciones de control de carácter físico-presupuestal.

Las acciones de carácter documental-administrativo, corresponde a acciones en donde se girarán de manera documental a través de oficios las indicaciones correspondientes a la descripción de la acción de control determinada para su atención, mismas que serán consideradas en un mediano plazo, y que su programación podrá considerarse dentro del presente ejercicio fiscal para su atención.

Y las acciones de control de carácter físico-presupuestal se consideran a largo plazo de conformidad a la solvencia presupuestaria municipal y serán estimadas en el ejercicio fiscal 2026 para su atención.



Tratamientos y Medidas de Seguridad.

Plan de Trabajo.

PLAN DE TRABAJO PARA LA IMPLEMENTACION DE MEDIDAS DE SEGURIDAD, DEL MUNICIPIO DE PACHUCA DE SOTO.

No.	Medida de Control	2026					2027											
		Ago	Sep	Oct	Nov	Dic	Ene	Feb	Mzo	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
I.- Medidas de Seguridad Administrativas																		
I.1	No dejar a la vista información personal.																	
I.1.1	Políticas de escritorio limpio																	
I.1.2	Hábitos de cierre y resguardo																	
I.1.3	Impresoras, escáneres, copiadoras y buzones limpios																	
I.2	Establecer Mecanismos para eliminar de manera segura la información																	
I.2.1	Destrucción segura de documentos																	
I.2.2	Borrar o eliminar la información en equipo de cómputo y medios de almacenamiento digital																	
I.2.3	Fijar periodos de resguardo y destrucción de información																	
I.2.4	Tomar precauciones en el uso de documentos reciclados																	
I.3	Documentar las responsabilidades en la protección de datos personales																	
I.3.1	Informar al personal sobre la importancia de la seguridad y protección de datos																	
I.3.2	Fomentar la cultura de la seguridad de la información																	
I.3.3	Difundir noticias en temas de seguridad																	
I.3.4	Asegurar la protección de datos personales en contrataciones																	
II.- Medidas de Seguridad Físicas																		
II.1	Establecer las medidas de seguridad en las áreas de trabajo																	
II.1.1	Resguardar el área de trabajo																	
II.1.2	Establecer bitácoras de registro para el personal ajeno al área de trabajo																	
II.1.3	Establecer bitácoras, para usuarios																	
II.2	Establecer medidas de seguridad para evitar robos.																	
II.2.1	Establecer Cerraduras y candados																	
II.2.2	Elementos preventivos disuasorios																	
II.3	Establecer medidas de seguridad para el movimiento de información entre áreas de trabajo.																	
II.3.1	Aprobación de salida de equipo de cómputo y/o medios de almacenamiento digital																	
II.3.2	Traslado de documentos																	
II.3.3	Usar mensajería certificada																	
III.- Medidas de Seguridad Técnicas																		
III.1	Actualización a los equipos de Cómputo.																	
III.1.1	Actualización del sistema operativo.																	
III.1.2	Actualización del software																	
III.1.3	Actualización del hardware																	
III.2	Actualización del software instalado en los equipos de Cómputo.																	
III.2.1	Uso de software actualizado																	
III.2.2	Restricción de uso de software distinto al Institucional																	
III.2.3	Mantenimiento preventivo																	
III.3	Medidas de Seguridad para el acceso al entorno de trabajo digital.																	
III.3.1	Uso de contraseñas y/o cifrado																	
III.3.2	Bloqueo y cierre de sesiones																	
III.3.3	Gestión de usuarios y accesos																	
III.4	Establecer medidas de seguridad para navegar en entornos digitales																	
III.4.1	Reglas de navegación segura																	
III.4.2	Reglas para la divulgación de información																	
III.4.3	Uso de conexiones seguras																	

Periodo de Ejecución



Tratamientos y Medidas de Seguridad.

Recomendación.

Por último es importante precisar que las dependencias y entidades de la Administración Pública Municipal, son las responsables de implementar las medidas de seguridad establecidas en el presente manual, el seguimiento y las acciones de mejora que puedan determinar los responsables de los tratamientos, deberán turnarlos a la Unidad de Transparencia para su análisis y valoración; este a su vez, lo presentara ante el Comité de Transparencia del Municipio de Pachuca de Soto, para su autorización, difusión y publicación de conformidad a lo establecido por las disposiciones legales en la materia.





GACETA MUNICIPAL

Para su consulta en:



Vía Web
www.pachuca.gob.mx



En las oficinas de:
Secretaría General Municipal
Oficialía Mayor del H. Ayuntamiento



Ubicadas en:
Plaza Gral. Pedro María Anaya No. 1, C.P. 42000
Col. Centro, Pachuca de Soto, Estado de Hidalgo.



Contacto
oficialia.mayor@pachuca.gob.mx

Tel. 71 71 500 ext. 1160