POLÍTICAS DE SEGURIDAD Y PROTECCIÓN DE DATOS PERSONALES

AYUNTAMIENTO

DE

TUXPAN

INTRODUCCIÓN

El presente documento tiene como objeto el de establecer las políticas que deberán de seguir los servidores públicos de este H. Ayuntamiento de Tuxpan, responsables del tratamiento y la protección de los datos personales que con motivo de su empleo, cargo o comisión traten.

Cada persona es propietaria de sus datos personales, por lo que cada persona tiene el derecho universal de autodeterminación o decisión respecto de sus datos personales, de tal manera que este H. Ayuntamiento y sus servidores públicos no tienen derecho de propiedad de los datos personales que en el ejercicio de sus atribuciones tratan, pero si la obligación legal para su protección.

El Ayuntamiento de Tuxpan está en el deber y en la responsabilidad de consagrar tiempo y recursos suficientes para asegurar que los activos de información estén suficientemente protegidos. Cuando ocurra un incidente grave que refleje alguna debilidad en los sistemas informáticos, se deberán tomar las acciones correctivas rápidamente para así reducir los riesgos. A todos los servidores públicos debe proporcionárseles adiestramiento, información, y advertencias para que ellos puedan proteger y manejar apropiadamente los recursos informáticos.

Los activos de información y los equipos informáticos son recursos importantes y vitales de nuestro Ayuntamiento de Tuxpan. Esto significa, que se deben tomar las acciones apropiadas para asegurar que la información y los sistemas informáticos estén apropiadamente protegidos de muchas clases de amenazas y riesgos tales como fraude, sabotaje, violación de la privacidad, intrusos, hackers, interrupción de servicio, accidentes y desastres naturales.

La finalidad de las políticas de seguridad que se describen más adelante es proporcionar instrucciones específicas sobre cómo mantener más seguros tanto los equipos de cómputo del Ayuntamiento de Tuxpan (conectados o no en red), como la información guardada en ellos, así la documentación física. La violación de dichas políticas puede acarrear medidas disciplinarias severas.

OBJETIVO

El H. Ayuntamiento de Tuxpan a través de las presentes políticas, tiene por objetivo implementar medidas de seguridad que garanticen la protección, tratamiento y conservación de los datos personales, recabados por las diferentes áreas que conforman este ente de gobierno municipal; a fin de determinar y difundir las vulnerabilidades, amenazas, riesgos que a nivel general son aplicables a los sistemas de información y áreas físicas en los que se manejan datos personales.

MARCO NORMATIVO

Ley número 316 de Datos Personales en Posesión de Sujetos Obligados para el Estado de Veracruz de Ignacio de la Llave.

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Lineamientos para la Tutela de los Datos Personales en el Estado de Veracruz.

EN QUE CONSISTE EL DERECHO DE LA PROTECCIÓN DE DATOS PERSONALES

El derecho a la protección de datos personales, consiste en buscar la protección de la persona en relación con el tratamiento de su información personal; el poder de disposición y control que faculta a su titular a decidir cuáles de sus datos proporciona a un tercero, así como el saber quién posee esos datos y para qué, pudiendo oponerse a esa posesión o uso.

TRATAMIENTO DE DATOS PERSONALES

Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos automatizados, informáticos, manuales, mecánicos, digitales o electrónicos, aplicados a los sistemas de datos personales, relacionados con la obtención, registro, organización, conservación, elaboración, utilización, cesión, difusión, cotejo o interconexión o cualquier otra forma que permita obtener información de los mismos y facilite al interesado el acceso, rectificación, cancelación u oposición de sus datos, así como su bloqueo, supresión o destrucción;

Por tal motivo, los responsables de las áreas del Ayuntamiento de Tuxpan para el tratamiento de datos personales, se conducirán bajo los principios y deberes de licitud, lealtad, información, consentimiento, finalidad, calidad, proporcionalidad, proporcionalidad, responsabilidad, seguridad y confiabilidad en términos de la Ley 316 de Datos Personales en Posesión del Sujeto Obligado y demás disposiciones normativas aplicables.

PRINCIPIOS Y DEBERES EN MATERIA DE DATOS PERSONALES:

- **Licitud:** El tratamiento de datos personales será lícito cuando el titular los entregue, previo consentimiento, o sea en cumplimiento de una atribución u obligación legal aplicable al sujeto obligado; en este caso, los datos personales recabados u obtenidos se tratarán por los medios previstos en el presente ordenamiento, y no podrán ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.

- **Lealtad:** El tratamiento de datos personales se realizará sin que medie dolo, engaño o medios fraudulentos, tengan un origen lícito, y no vulneren la confianza del titular.

- **Información:** El Responsable deberá informar al titular de los datos sobre las características principales del tratamiento, la finalidad y cualquier cambio del estado relacionados con sus datos personales.

- **Consentimiento:** Toda manifestación previa, de voluntad libre, específica, informada e inequívoca por la que el titular acepta, mediante declaración o acción afirmativa, el tratamiento de sus datos personales.

- **Finalidad:** Los datos personales recabados y tratados tendrán fines determinados, explícitos y legítimos y no podrán ser tratados ulteriormente con fines distintos para los que fueron recabados. Los datos personales con fines de archivo de interés público, investigación científica e histórica, o estadísticos no se considerarán incompatibles con la finalidad inicial. La finalidad incluirá el ciclo de vida del dato personal, de tal manera, que concluida ésta, los datos puedan ser suprimidos, cancelados o destruidos.

- **Calidad:** Los datos personales deben ser ciertos, adecuados, pertinentes y proporcionales, no excesivos, en relación con el ámbito y la finalidad para la que fueron recabados.

- **Proporcionalidad:** El responsable tratara sólo aquellos datos personales que resulten necesarios, adecuados y relevantes en relación con la finalidad o finalidades, para lo cual se obtuvieron.

- **Responsabilidad:** El responsable debe tomar las medidas necesarias para cumplir con los principios y obligaciones antes señaladas, entre ellas esquemas de autorregulación, que les ayude a mejorar el tratamiento y cuidado de los datos personales.

- **Seguridad:** Los responsables están obligados a resguardar los datos personales en bases de datos protegidas con medidas de seguridad que eviten daño, pérdida, alteración o destrucción de los datos personales, o su uso, acceso o tratamiento no autorizado.

- **Confidencialidad:** El responsable garantizará que exclusivamente el titular pueda acceder a sus datos, o en su caso, el mismo Responsable y el usuario a fin de cumplir con las finalidades del tratamiento. En cualquier caso, se deberá garantizar la secrecía y la no difusión de los mismos. Sólo el titular podrá autorizar la difusión de sus datos personales.

CATEGORÍAS DE LOS DATOS PERSONALES

TIPOS DE DATOS PERSONALES, NIVEL DE PROTECCIÓN

Datos identificativos (BÁSICO).- El nombre, domicilio, teléfono particular, teléfono celular, firma, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), Clave de elector, Matrícula del Servicio Militar Nacional, número de pasaporte, lugar y fecha de nacimiento, nacionalidad, edad, fotografía y demás análogos.

Datos electrónicos (BÁSICO).- Las direcciones electrónicas, tales como, el correo electrónico no oficial, dirección IP (Protocolo de Internet), dirección MAC (dirección Media Access Control o dirección de control de acceso al medio), así como el nombre del usuario, contraseñas, firma electrónica; o cualquier otra información empleada por la persona, para su identificación en Internet, acceso a sistemas de información u otra red de comunicaciones electrónicas y demás análogos.

Datos laborales (BÁSICO).- Documentos de reclutamiento y selección, nombramiento, incidencia, capacitación, actividades extracurriculares, referencias laborales, referencias personales, solicitud de empleo, hoja de servicio y demás análogos.

Datos académicos (BÁSICO).- Trayectoria educativa, calificaciones, títulos, cédula profesional, certificados y reconocimientos y demás análogos.

Datos de salud (ALTO).- El expediente clínico de cualquier atención médica, referencias o descripción de sintomatologías, detección de enfermedades, incapacidades médicas, discapacidades, intervenciones quirúrgicas, vacunas,

consumo de estupefacientes, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, así como el estado físico o mental de la persona y demás análogos.

Datos patrimoniales (MEDIO).- Los correspondientes a bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, fianzas, servicios contratados, referencias personales y demás análogos.

Datos sobre procedimientos administrativos (MEDIO).- La información relativa una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal, fiscal, administrativa o de cualquier otra rama del Derecho.

Datos de tránsito y movimientos migratorios (BÁSICO).- Información relativa al tránsito de las personas dentro y fuera del país, así como información migratoria.

Datos biométricos (ALTO).- Huellas dactilares, ADN, geometría de la mano, características de iris y retina y demás análogos.

Datos sensibles (ALTO).- Origen étnico o racial, características morales o emocionales, ideología y opiniones políticas, creencias, convicciones religiosas, filosóficas, la pertenencia a sindicatos, la salud y preferencia sexual y demás análogos.

Datos personales de naturaleza pública (BÁSICO).- Aquellos que por mandato legal sean accesibles al público.

LAS MEDIDAS DE SEGURIDAD ADOPTADAS POR EL RESPONSABLE, DEBERÁN CONSIDERAR LO SIGUIENTE:

I. El riesgo inherente a los datos personales tratados;

II. La sensibilidad de los datos personales tratados;

III. El desarrollo tecnológico;

IV. Las posibles consecuencias de una vulneración para los titulares;

V. Las transferencias de datos personales que se realicen;

VI. El número de titulares;

VII. Las vulneraciones previas ocurridas en los sistemas de tratamiento; y

VIII. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.

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.

Además de las que señalen las leyes respectivas y la normatividad aplicable, se considerarán como vulneraciones de seguridades directas o indirectas, en cualquier fase del tratamiento de datos, al menos, las siguientes:

I. La pérdida o destrucción no autorizada;

II. El robo, extravío o copia no autorizada;

III. El uso, acceso o tratamiento no autorizado; o

IV. El daño, la alteración o modificación no autorizada.

POLÍTICAS EN MATERIA DE SEGURIDAD DE DATOS PERSONALES FÍSICAS.

Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, los principales rubros de mayor relevancia a considerar conforme al tratamiento de datos personales, son las siguientes actividades:

1. Concentrar los archivos físicos que contiene datos personales en lugares aislados, preferentemente en las oficinas principales de los titulares de áreas.
2. Procurar solicitar la instalación de chapas con llave a fin de limitar el acceso de personas.
3. Procurar en la medida de lo posible transferir de archivos físicos a bases electrónicas, además de elevar el nivel de seguridad, permitirá la perdida de información con motivo de amenazas del tipo no intencionales.
4. Limitar el número de personas que tengan acceso a archivos físicos.
5. Realizar un registro interno de personas que ingresan a las oficinas que contienen datos personas en archivos físicos.
6. Procurar suscribir acuerdos de confidencialidad con el personal que maneje datos personales.
7. Reportar inmediatamente a la Unidad de Transparencia de cualquier robo o extravió de documentos que contengan datos personales.

8. Reportar inmediatamente a la Unidad de Transparencia sobre los cambios de personal que manejen archivos físicos que contengan datos personales.

POLÍTICAS EN MATERIA DE SEGURIDAD DE DATOS PERSONALES DIGITALES.

Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y recursos involucrados en su tratamiento. Las siguientes políticas enmarcan los principales rubros de mayor relevancia a considerar, conforme al tratamiento de datos personales y son:

1. Utilizar claves de usuario y contraseñas de usuario de manera exclusivamente personal, así como no compartirlas, prestarlas ni mantenerlas anotadas a la vista de otras personas.

2. Establecer y utilizar contraseñas robustas, es decir, de al menos ocho caracteres alfanuméricos, evitando que sean iguales al nombre del usuario, o cualquier otro nombre de personas, considerando que estas sean fáciles de recordar y difíciles de adivinar o descifrar por un tercero, a fin de salvaguardar la información y datos personales a los que se tenga acceso.

3. Notificar de manera inmediata a la Coordinación de Tecnologías de la Información y Comunicación, los casos en los que los usuarios identifiquen o consideren que sus claves de usuario y/o contraseñas han sido utilizadas por un tercero, a fin de evitar pérdida, robo, eliminación o alteración de información que contenga datos personales, así como asignar una nueva contraseña o clave.

4. Utilizar el correo electrónico institucional para fines relacionados con las actividades laborales, evitando enviar datos personales o hacerlo asignando una contraseña a fin de procurar su protección.

5. Mantener los documentos electrónicos y físicos en lugares seguros, bajo llave, dentro de cajones cerrados, o bajo la protección de alguna contraseña, a fin de promover la restricción a los datos personales que pudieran contener.

6. No difundir, transmitir, ni compartir documentos electrónicos ni físicos que contengan datos personales en dispositivos móviles (celulares, tabletas o laptos), a fin de garantizar que estos no sean divulgados de manera no autorizada.

7. Evitar dejar u olvidar los documentos físicos que contengan datos personales en los equipos de impresión, así como evitar su impresión, escaneo y fotocopiado si no es realmente requerido para las actividades laborales.

8. Procurar solicitar acceso a los sistemas de información de tratamiento de datos personales, bajo el precepto del mínimo privilegio, es decir, únicamente al personal que por sus funciones y facultades laborales los requiera, a fin de mantener una adecuada segregación de funciones, restricción de acceso y tratamiento de esos datos.

9. Triturar todos los documentos físicos que contengan datos personales y ya no sean útiles y/o necesarios para las actividades laborales, así como borrar o eliminar de la papelera de reciclaje del escritorio de los equipos de cómputo, los documentos o archivos electrónicos que recaen en esa misma situación, garantizando la completa eliminación de los datos personales que ya no sean necesario de tratar en esos medios.

10. Notificar las bajas de accesos a los sistemas de información de tratamiento de datos personales, con oportunidad, en cuanto sean del conocimiento de los responsables de las áreas, a fin de restringir

el acceso a dichos datos por personal no autorizado y que ya no forma parte del Ayuntamiento de Tuxpan.

Será obligación de todo el personal de cada una de las áreas del Ayuntamiento de Tuxpan el proteger y resguardar debidamente la información que contenga Datos Personales, para lo cual deberán de tomar todas las medidas que sean necesarias para evitar que la información o documentos que se encuentran bajo su custodia o de sus personas, servidores públicos o de quienes tengan acceso o conocimiento con motivo de su empleo, cargo o comisión, se haga mal uso de esta, la sustraigan, divulguen, alteren o destruyan, sin causa legítima, además de asegurar su custodia, conservación, integridad y disponibilidad.

PRINCIPIOS GENERALES PARA LA PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DEL AYUNTAMIENTO DE TUXPAN.

1. En el tratamiento de datos personales, las Unidades Administrativas y los servidores públicos vinculados deberán observar los principios de calidad, consentimiento, finalidad, información, lealtad, licitud, proporcionalidad, y responsabilidad.

2. Las Unidades Administrativas a través de sus titulares y los servidores públicos vinculados, deberán adoptar las medidas necesarias para mantener exactos, completos, pertinentes, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos, para lo cual deberán atender lo siguiente:

I. Los datos personales son exactos cuando reflejan la realidad de la situación de su titular, es decir, son verdaderos o fieles;
II. Los datos personales están completos cuando no falta ninguno de los que se requiera para las finalidades para las cuales se obtuvieron y son tratados;
III. Los datos personales son pertinentes cuando corresponden efectivamente al titular y no a una homonimia;

IV. Los datos personales están actualizados cuando corresponden a la situación presente de su titular; y
V. Los datos personales son correctos cuando cumplen con todas las características anteriores, es decir, son exactos, completos, pertinentes y actualizados.

3. Cada Unidad Administrativa designará un servidor público vinculado del o los Sistemas de Datos Personales, quién será el encargado de apoyar al Titular de la Unidad Administrativa de su adscripción para realizar lo establecido en las presentes Políticas y tendrá las siguientes funciones:

I. Adoptar las medidas de seguridad para el resguardo del o los Sistemas de Datos Personales bajo su responsabilidad, en soporte físico, de manera que se evite su alteración, pérdida o acceso no autorizado;

II. Autorizar expresamente, en los casos en que no esté previsto por un instrumento jurídico o disposición normativa, a los usuarios, y llevar una relación actualizada de las personas que tengan acceso al o los Sistemas de Datos Personales que se encuentran en soporte físico, y

III. Aplicar y vigilar el cumplimiento de las medidas y estándares de seguridad para la conservación y resguardo de Sistemas de Datos Personales del Ayuntamiento de Tuxpan, que para tal efecto determine el Comité, a través de las disposiciones normativas específicas de observancia general para las Unidades Administrativas que cuenten con los referidos Sistemas.

4. Las Unidades Administrativas deberán tratar los datos personales que resulten estrictamente necesarios para el ejercicio de sus atribuciones y funciones, observando las disposiciones aplicables en materia de datos personales.

5. Los servidores públicos vinculados están obligados en todo momento a garantizar las condiciones y requisitos necesarios para el adecuado tratamiento, así como la debida administración y custodia de los datos personales que se encuentren bajo su resguardo, con el objeto de maximizar el ejercicio de los derechos ARCO.

6. Será confidencial la Información que contenga Datos Personales.

Los Datos Personales Sensibles, son aquellos que el Ayuntamiento de Tuxpan, en sus archivos, concernientes a una persona física identificada o identificable, que permiten conocer datos relativos a la vida privada y a la intimidad de las personas y que se describen a continuación de manera enunciativa y no limitativa:

I. Origen racial o étnico;
II. Estado de salud presente o futuro;
III. Información genética;
IV. Creencias religiosas;
V. Creencias filosóficas y morales;
VI. Opiniones políticas;
VII. Preferencia sexual, y
VIII. Otros ascciados.

7. Los Datos Personales serán confidenciales, independientemente de que hayan sido obtenidos por el Ayuntamiento de Tuxpan directamente de su titular o por cualquier otro medio.

8. El Ayuntamiento de Tuxpan para el tratamiento de datos personales, se observarán los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales, en términos de la Ley número 316 de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Veracruz de Ignacio de la Llave, Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás disposiciones normativas aplicables.

El servidor público del Ayuntamiento de Tuxpan, encargado de recabar el consentimiento del titular de los datos personales para la transferencia de los mismos, deberá entregar a éste, en forma previa a cada transmisión, la información suficiente acerca de las implicaciones de otorgar, de ser el caso, su consentimiento.

9. Para el ejercicio de los derechos ARCO será necesario acreditar la identidad del titular y, en su caso, la identidad y personalidad con la que actúe el representante.

El ejercicio de los derechos ARCO por persona distinta a su titular o a su representante, será posible, excepcionalmente, en aquellos supuestos previstos por disposición legal, o en su caso, por mandato judicial.

Tratándose de datos personales concernientes a personas fallecidas, la persona que acredite tener un interés jurídico, de conformidad con las leyes aplicables, podrá ejercer los derechos que le confiere el presente Capítulo, siempre que el titular de los derechos hubiere expresado fehacientemente su voluntad en tal sentido o que exista un mandato judicial para dicho efecto.

En los casos en que el ejercicio de los derechos ARCO de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad, de conformidad con las leyes civiles, se estará a las reglas de representación dispuestas en la misma legislación.

10. La Unidad de Transparencia deberá elaborar un inventario actualizado de aquellos Sistemas de Datos Personales con los que cuente el Ayuntamiento de Tuxpan.

Cada Unidad Administrativa responsable de un Sistema de Datos Personales deberá adoptar las medidas necesarias para mantener seguros, exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos.

Se presume que se cumple con la calidad en los datos personales cuando son proporcionados directamente por el titular y hasta que éste no manifieste y acredite lo contrario.

Cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones que resulten aplicables, deberán ser suprimidos, previo bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos.

Los plazos de conservación de los datos personales no deberán exceder aquellos que sean necesarios para el cumplimiento de las finalidades que justificaron su tratamiento, y deberán atender a las disposiciones aplicables en la materia de que se trate y considerar los aspectos administrativos, contables, fiscales, jurídicos e históricos de los datos personales.

Las actualizaciones de los Sistemas de Datos Personales deberán realizarse por las Unidades Administrativas responsables de su administración, el Titular de éstas, remitirá a la Unidad de Transparencia en el formato que establezca para tal efecto la modificación, actualización o cancelación de dichos Sistemas.

Las Unidades Administrativas responsables de Sistemas de Datos Personales deberán establecer y documentar los procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales que lleven a cabo, en los cuales se incluyan los periodos de conservación de los mismos.

En los procedimientos a que se refiere el párrafo anterior, las Unidades Administrativas responsables de Sistemas de Datos Personales deberán incluir mecanismos que le permitan cumplir con los plazos fijados para la supresión de los datos personales, así como para realizar una revisión periódica sobre la necesidad de conservar los datos personales en el Ayuntamiento de Tuxpan.

11. Corresponderá al Titular de la Unidad Administrativa responsable establecer controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales, guarden confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar su relación con el mismo.

Lo anterior, sin menoscabo de lo establecido en las disposiciones de acceso a la información pública.

Con independencia del tipo de sistema en el que se encuentren los Datos Personales o el tipo de tratamiento que se efectúe, el Titular de la Unidad Administrativa responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico pudiendo solicitar apoyo de la Coordinación de Tecnologías de la Información y Comunicación para la protección

de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;

b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;

c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y

d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

e) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;

f) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;

g) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y

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

12. En el momento en que se recaben datos personales, cada Unidad Administrativa deberá hacer del conocimiento del titular de los datos, tanto en los formatos físicos como en los medios electrónicos utilizados para ese fin, el aviso de privacidad, el cual precisará la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto. Para que el aviso de privacidad cumpla de manera eficiente con su función de informar, deberá estar redactado y estructurado de manera clara y sencilla.

14. Para informar al titular de los datos personales que obren en Sistemas de Datos Personales que las Unidades Administrativas del Ayuntamiento de Tuxpan resguarden en ejercicio de atribuciones y funciones relativas a información

correspondiente a su gestión administrativa, deberá ponerse a su disposición el Aviso de Privacidad en dos modalidades: simplificado e integral.

El aviso simplificado deberá contener al menos la siguiente información:

I. Denominación del Ayuntamiento de Tuxpan y de la Unidad Administrativa responsable;
II. Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieran el consentimiento del titular;
III. Cuando se realicen transferencias de datos personales que requieran consentimiento, se deberá informar:
a. Las autoridades, poderes, entidades, órganos y organismos gubernamentales y las personas físicas o morales a las que se transfieren los datos personales, y
b. Las finalidades de estas transferencias;
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.

La puesta a disposición del aviso de privacidad al que refiere, no exime a la Unidad Administrativa responsable de su obligación de proveer los mecanismos para que el titular pueda conocer el contenido del aviso de privacidad al que se refiere el artículo siguiente.

Los mecanismos y medios a los que se refiere el apartado IV, deberán estar disponibles para que el titular pueda manifestar su negativa al tratamiento de sus datos personales para las finalidades o transferencias que requieran el consentimiento del titular, previo a que ocurra dicho tratamiento.

16. El Aviso de Privacidad integral al que refiere el apartado V, además de lo dispuesto en los apartados que lo preceden, deberá contener, al menos, la siguiente información:
I. El domicilio del Ayuntamiento de Tuxpan;
II. Los datos personales que serán sometidos a tratamiento, identificando aquéllos que son sensibles;

III. El fundamento legal que faculta al responsable para llevar a cabo el tratamiento;

IV. Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieren el consentimiento del titular;

V. Los mecanismos, medios y procedimientos disponibles para ejercer los derechos ARCO;

VI. El domicilio de la Unidad de Transparencia, y

VII. Los medios a través de los cuales se comunicará a los titulares los cambios al aviso de privacidad.

RECOMENDACIONES:

SEGURIDAD DE DATOS PERSONALES

Destruye los documentos cuando hayan dejado de ser necesarios

- ✓ **Evita tirar documentos con datos personales sin triturar.**
- ✓ **No dejar documentos en la fotocopiadora.**
- ✓ **Cuidar el reúso de papel con datos personales.**
- ✓ **No dejar a la vista datos personales**

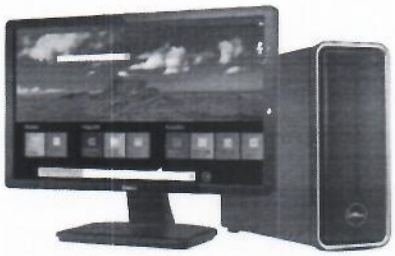
UNIDAD DE TRANSPARENGIA

SEGURIDAD DE DATOS PERSONALES
Recomendaciones

- ✓ Evita dejar documentos a la mano.
- ✓ Resguarda tus contraseñas en un lugar seguro.
- ✓ Usar archiveros con llave.

UNIDAD DE TRANSPARENCIA

SEGURIDAD DE DATOS PERSONALES
Recomendaciones



- ✓ **NO DEJES ABIERTA TU CUENTA EN TU PC.**
- ✓ **UTILIZA CONTRASEÑA DE ACCESO**
- ✓ **CONFIGURA LA SUSPENSIÓN DE ACTIVIDAD DESPUÉS DE 10 MINUTOS INACTIVO**

UNIDAD DE TRANSPARENCIA

GLOSARIO

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;

Aviso de privacidad: Documento físico, electrónico o en cualquier 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;

Bases de Datos: Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionado a criterios determinados con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización;

Bloqueo: La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho período, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda;

Comité: El Comité de Transparencia de cada sujeto obligado en el Estado, a que hacen referencia los artículos 43 de la Ley General y 130 de esta Ley;

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

Datos personales: Cualquier información concerniente a una persona física 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 éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud, información genética, datos biométricos, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;

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

Encargado: La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales por cuenta del responsable;

Ley: Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Veracruz;

Ley General: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;

Medidas compensatorias: Mecanismos alternos para dar a conocer a los titulares el aviso de privacidad, a través de su difusión por medios masivos de comunicación u otros de amplio alcance;

Medidas de seguridad: conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten garantizar la protección, confidencialidad, disponibilidad e integridad de los datos personales;

Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificacion, clasificación y borrado seguro de la información, así como la sensibilización, formación y capacitación del personal, en materia de protección de datos personales;

Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento

Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y recursos involucrados en su tratamiento.

Responsable: Cualquier autoridad, dependencia, entidad, órgano y organismo de los poderes Legislativo, Ejecutivo y Judicial, ayuntamientos, órganos, organismos constitucionales autónomos, tribunales administrativos, fideicomisos y fondos públicos y partidos políticos del Estado, que decide y determina los fines, medios y demás cuestiones relacionadas con determinado tratamiento de datos personales, es decir, aquellos que tengan carácter de sujeto obligado.

Sistema de datos personales: Los datos personales contenidos en los archivos de un sujeto obligado que puede comprender el tratamiento de una o diversas bases de datos para el cumplimiento de una o diversas finalidades.

Supresión: La baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los

datos personales bajo las medidas de seguridad previamente establecidas por el responsable;

Titular: Persona física a quien pertenecen los datos personales;

Tratamiento: De manera enunciativa más no limitativa 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 que funge como vínculo entre el responsable y el titular.