INSTITUTO MUNICIPAL DE LA JUVENTUD EN TLAQUEPAQUE

Documento de Seguridad para Sistemas de Datos Personales

30 de Octubre del 2017

OBJETIVOS.

Describir el proceso de la administración de seguridad física y las normas comprendidas en la materia, con referencia a la guía para la elaboración de un documento de sistemas de seguridad de datos personales y la elaboración de especificaciones, guías, procedimientos generales, instrucciones de trabajo y registros de control.

MARCO JURÍDICO.

Artículo 2, 3, 20, 21, 22 y 23 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. Capítulo II Sección Segunda del Reglamento de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. Así como a lo establecido por las recomendaciones en Materia de Seguridad de Datos Personales, y por lo dispuesto dentro de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, la Ley Federal de Archivos, los Lineamientos para la Organización y Conservación de Archivos, y el Reglamento del Instituto Municipal de la Juventud en San Pedro Tlaquepaque.

NIVELES DE PROTECCIÓN DE LOS DATOS PERSONALES.

a) Nivel estándar
Esta categoría considera información de identificación, contacto, datos laborales y académicos de una persona física identificada o identificable, tal como: nombre, teléfono, edad, sexo, RFC, CURP, estado civil, dirección de correo electrónico, lugar y fecha de nacimiento, nacionalidad, puesto de trabajo, lugar de trabajo, experiencia laboral, datos de contacto laborales, idioma o lengua, escolaridad, trayectoria educativa, títulos, certificados, cédula profesional, entre otros.

b) Nivel sensible
Esta categoría contempla los datos que permiten conocer la ubicación física de la persona, tales como la dirección física e información relativa al tránsito de las personas dentro y fuera del país.

También son datos de nivel sensible aquéllos que permitan inferir el patrimonio de una persona, que incluye entre otros, los saldos bancarios, estados y/o número de cuenta, cuentas de inversión, bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos, egresos, buró de crédito, seguros, afores y fianzas. Incluye el número de tarjeta bancaria de crédito y/o débito.

Son considerados también los datos de autenticación con información referente a los usuarios, contraseñas, información biométrica (huellas dactilares, iris, voz, entre otros), firma autógrafa y electrónica y cualquier otro que permita autenticar a una persona.

Dentro de esta categoría se toman en cuenta los datos jurídicos tales como antecedentes penales, amparos, demandas, contratos, litigios y cualquier otro tipo de información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa.

Finalmente, se contemplan los datos personales sensibles de la Ley, es decir, aquéllos que afecten a la esfera más íntima de su titular. Por ejemplo, se consideran sensibles los que puedan revelar aspectos como origen racial o étnico, estado de salud pasado, presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical,

opiniones políticas, preferencia sexual, hábitos sexuales y cualquier otro cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave a la integridad del titular.

c) Nivel especial

Los datos de nivel especial son los que de acuerdo a su naturaleza y contexto pueden causar un daño excepcional a los titulares, por ejemplo:

Información adicional de tarjeta bancaria que considera el número de la tarjeta de crédito y/o débito mencionado anteriormente en combinación con cualquier otro dato relacionado o contenido en la misma, por ejemplo fecha de vencimiento, códigos de seguridad, datos de banda magnética o número de identificación personal (PIN).

Los datos personales de titulares de alto riesgo, cuya profesión, oficio o condición los expone a una mayor probabilidad de ser atacados debido al beneficio económico o reputacional que su información representa para una persona no autorizada. Por ejemplo, líderes políticos, religiosos, empresariales, de opinión y cualquier otra persona que sea considerada como personaje público. Asimismo, se considera a cualquier persona cuya profesión esté relacionada con la impartición de justicia y seguridad nacional.

LA TABLA CONTIENE LA CLASIFICACIÓN POR NIVEL DE ALGUNOS TIPOS DE DATO:

Tipo de dato	Nivel
Información adicional al número de tarjeta bancaria	Especial
Titulares de alto riesgo	Especial
Ubicación física	Sensible
Patrimonio	Sensible
Autenticación	Sensible
Jurídicos	Sensible
Salud, creencias, opiniones políticas	Sensible
Identificación y contacto	Estándar

TIPO DE TRANSMISIONES DE DATOS PERSONALES Y MODALIDADES PARA LA TRANSMISIÓN

Se considerar tres tipos de transmisiones que se pueden llevar a cabo dependiendo de quién sea el destinatario:

a) Interinstitucionales: Transmisiones de datos a dependencias y entidades de la Administración Pública Municipal, de los poderes Legislativo, Ejecutivo y Judicial locales de las entidades federativas o Gubernamentales, en el ejercicio de sus facultades.

b) Con entes privados u organizaciones civiles: Para implementar las medidas de seguridad aplicables a las transmisiones citadas, la Unidad Administrativa responsable, debe considerar la modalidad por la cual se envían los datos personales a los destinatarios, pudiendo hacerse mediante el traslado de soportes físicos, mediante el traslado físico de soportes electrónicos o el traslado sobre redes electrónicas.

Cada una de estas modalidades se deberá ceñir a lo siguiente:

a) Traslado de soportes físicos: En esta modalidad los datos personales se trasladan en medios de almacenamiento inteligibles a simple vista que no requieren de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos. Ejemplo del traslado de soportes físicos es cuando una dependencia envía por correspondencia oficios o formularios impresos.

b) Traslado físico de soportes electrónicos: En esta modalidad se trasladan físicamente para entregar al destinatario los datos personales en archivos electrónicos contenidos en medios de almacenamiento inteligibles sólo mediante el uso de algún aparato con circuitos electrónicos que procese su contenido para examinar, modificar o almacenar los datos. Ejemplo de ello es cuando una dependencia entrega a otra por mensajería oficial un archivo electrónico con datos personales contenidos en discos flexibles, discos compactos o dispositivos de memoria USB, entre otros.

c) Traslado sobre redes electrónicas: En esta modalidad se transmiten los datos personales en archivos electrónicos mediante una red electrónica. Por ejemplo, cuando un archivo electrónico con un listado de beneficiarios se envía de una dependencia a otra por Internet.

DISPOSICIÓN FINAL DE LOS DOCUMENTOS CON DATOS PERSONALES.

a) Tiempo de conservación de los datos: Los datos personales del solicitante, serán conservados bajo el sistema de archivo correspondiente a su ciclo vital del expediente (tramite, conservación o histórico), bajo el sistema de reserva.

b) Destino final de los datos personales: Existen cuatro tipos de disposición final del documento

- Resguardo y conservación de los documentos físicos y/o electrónicos.

- Supresión de los datos personales en los documentos físicos y/o electrónicos. (se establecerá el destino de los datos contenidos o las previsiones que se adopten para su destrucción).

- Destrucción de los documentos físicos y/o electrónicos, conservando solo la información útil para finalidades estadísticas o históricas, previamente sometidos al procedimiento de disociación.

- Destrucción de los documentos físicos y/o electrónicos.

IMJUVET
Instituto Municipal de la Juventud Tlaquepaque

SISTEMA DE DATOS PERSONALES

DATOS DEL SUJETO OBLIGADO.			
Fecha de Elaboración.	**Día**	**Mes**	**Año**
Sujeto Obligado.			
Unidades Administrativas Responsables.			

DIRECCIÓN GENERAL	**RESPONSABLE**	**CARGO**
DOMICILIO	**TELÉFONO**	**CORREO ELECTRÓNICO**
ÁREA RESPONSABLE	**ENCARGADO DEL ÁREA RESPONSABLE**	**NOMBRAMIENTO**

DATOS GENERALES DEL SISTEMA.		
Finalidad de sistemas y los usos previstos.		
Las personas o grupos de personas sobre las cuales se obtienen los datos.		
Procedimiento de recolección y actualización de datos		
Tipo de datos personales	☐ Estándar ☐ Sensible ☐ Especial	Nombre completo, domicilio, teléfono particular, teléfono celular, correo electrónico y firma autógrafa.
Tipo de tratamiento		

ACCIONES PARA LA SEGURIDAD DE LOS DATOS PERSONALES.	
Unidades internas, sujetos obligados, autoridades o terceros a los que en su caso se ceden los datos.	**Finalidad**

<table>
<tr><td rowspan="3">Nivel de protección exigible.</td><td>☐ Básico</td><td rowspan="3">☐ Transmisiones de datos personales
☐ Resguardo de sistemas de datos personales con soportes físicos
☐ Bitácoras para accesos y operación cotidiana
☐ Registro de incidentes
☐ Acceso a las instalaciones
☐ Actualización del sistema de datos personales
☐ Perfiles de usuario y contraseñas
☐ Procedimientos de respaldo y recuperación de datos</td></tr>
<tr><td>☐ Medio</td></tr>
<tr><td>☐ Alto</td></tr>
<tr><td colspan="3">DISPOSICIÓN FINAL DE LOS DOCUMENTOS CON DATOS PERSONALES.</td></tr>
<tr><td>Tiempo de conservación de los datos.</td><td colspan="2">Los datos personales del solicitante, serán conservados bajo el sistema de archivo correspondiente a su ciclo vital del expediente (tramite, conservación o histórico), bajo el sistema de reserva.</td></tr>
<tr><td>Destino final de los datos personales</td><td colspan="2">☐ Resguardo y conservación de los documentos físicos y/o electrónicos.
☐ Supresión de los datos personales en los documentos físicos y/o electrónicos. (se establecerá el destino de los datos contenidos o las previsiones que se adopten para su destrucción).
☐ Destrucción de los documentos físicos y/o electrónicos, conservando solo la información útil para finalidades estadísticas o históricas, previamente sometidos al procedimiento de disociación.
☐ Destrucción de los documentos físicos y/o electrónicos.</td></tr>
<tr><td colspan="3">DERECHOS ARCO</td></tr>
<tr><td colspan="3">Si desea ejercer sus Derechos de Acceso, Rectificación, Cancelación y Oposición de la información de Datos Personales que el Instituto Municipal de la Juventud en San Pedro Tlaquepaque; puede presentarse a las oficinas del IMJUVET ubicadas en Prolongación Pedro de Loza 195, Colonia Hidalgo, Municipio de San Pedro Tlaquepaque, Jalisco CP 45540. Tel. 36575200
Mayor información sobre los Derechos ARCO: https://imjuve.tlaquepaque.gob.mx/wp-content/uploads/2016/05/Gu%C3%ADa-DerechosARCO-SOLICITUD.pdf</td></tr>
<tr><td colspan="3">FUNDAMENTACIÓN</td></tr>
<tr><td colspan="3">Artículo 2, 3, 20, 21, 22 y 23 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. Capítulo II Sección Segunda del Reglamento de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. Así como a lo establecido por las recomendaciones en Materia de Seguridad de Datos Personales, y por lo dispuesto dentro de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, la Ley Federal de Archivos, los Lineamientos para la Organización y Conservación de Archivos, y el Reglamento del Instituto Municipal de la Juventud en San Pedro Tlaquepaque.</td></tr>
</table>