Políticas Internas de Gestión y Tratamiento de Datos Personales

En el cumplimiento de las atribuciones y objeto reconocidos en nuestra Ley Orgánica, todas las Unidades Administrativas del Instituto de Información Estadística y Geográfica del Estado de Jalisco, recaban directa o indirectamente Datos Personales tanto de sus trabajadores como de terceras personas, que terminan en posesión del sujeto obligado, por lo tanto, es importante determinar el tratamiento correcto de los mismos, protegerlos, y así mantener tanto nuestros datos personales como los de terceros protegidos. El presente documento tiene como finalidad dar cumplimiento a las obligaciones reconocidas en los artículos 30, 31, 32 fracción I, y 33 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

Artículo 1.- Las presentes políticas son de aplicación y observancia general para todos los servidores públicos del Instituto de Información Estadística y Geográfica del Estado de Jalisco, con la finalidad de garantizar la confidencialidad, integridad y disponibilidad de los datos personales en posesión de este sujeto obligado, cada director de Unidad Administrativa o Área, deberá aplicar las presentes políticas.

Artículo 2.- Para efectos de estas políticas, se entenderá por:

I. **Área(s):** Cada una de las Unidades Administrativas reconocidas en el Estatuto Orgánico del Instituto de Información Estadística y Geográfica del Estado de Jalisco, así como las que se hayan creado a la fecha, incluyendo el Órgano Interno de Control.

II. **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;

III. **Bloqueo:** La identificación y conservación de los 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 correspondiente. Durante dicho período los datos personales no podrán ser objeto de tratamiento y concluido éste se deberá proceder a la supresión en la base de datos, archivo, registro, expediente o sistema de información que corresponda;

IV. **Comité:** El Comité de Transparencia del Instituto de Información Estadística y Geográfica del Estado de Jalisco.

V. **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;

VI. **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;

VII. **Disociación:** El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo;

VIII. **Evaluación de impacto en la protección de datos personales:** documento mediante el cual se valoran y determinan los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar, prevenir y mitigar posibles riesgos que puedan comprometer el cumplimiento de los principios, deberes, derechos y demás obligaciones previstas en esta Ley y demás disposiciones aplicables;

IX. **IIEG:** Instituto de Información Estadística y Geográfica del Estado de Jalisco.

X. **Ley:** Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Jalisco y sus Municipios;

XI. **Servidor Público:** Todos los servidores públicos del IIEG que formen parte de la plantilla de personal.

XII. **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;

XIII. **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

XIV. **Unidad:** Unidad de Transparencia del Instituto de Información Estadística y Geográfica del Estado de Jalisco.

Artículo 3.- Las áreas del IIEG deberán implementar las medidas necesarias para preservar la confidencialidad, integridad y disponibilidad de los Datos Personales que se encuentren en su posesión.

Capítulo I
Principios

Artículo 4.- Principio de observancia. Todos los servidores públicos del IIEG deberán observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, y proporcionalidad en el tratamiento de los datos personales.

Artículo 5.- Principio de Licitud. Sera lícito el tratamiento de datos personales cuando sea exclusivamente en observancia a las facultades o atribuciones que la normatividad aplicable les confiera y deberán obtenerse a través de los medios previstos en dichas disposiciones.

Artículo 6.- Principio de Finalidad. Todo tratamiento de datos personales que efectúen los servidores públicos del IIEG, deberá estar justificado por finalidades concretas, explícitas, lícitas y legítimas y deberá sujetarse a los principios contenidos en el presente capítulo, relacionadas con las facultades y atribuciones que la normatividad aplicable les confiera.

Se entenderá que las finalidades son:

I. Concretas: cuando el tratamiento de los datos personales atiende a la consecución de fines específicos o determinados, sin que sea posible la existencia de finalidades genéricas que puedan generar confusión en el titular;

II. Explícitas: cuando las finalidades se expresan y dan a conocer de manera clara en el aviso de privacidad, y

III. Lícitas y legítimas: cuando las finalidades que justifican el tratamiento de los datos personales son acordes con las atribuciones expresas del responsable, conforme a lo previsto en la legislación mexicana y el derecho internacional aplicable.

Solamente se podrá tratar datos personales para finalidades distintas a aquellas establecidas en el aviso de privacidad, siempre y cuando cuente con atribuciones conferidas en la ley y medie el consentimiento del titular, salvo que sea una persona reportada como desaparecida, en los términos previstos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Jalisco y demás disposiciones aplicables.

Artículo 7.- Principio de Lealtad. Los servidores públicos del IIEG, no deberán obtener y tratar datos personales a través de medios engañosos o fraudulentos; deberán privilegiar la protección de los intereses del titular y la expectativa razonable de privacidad.

Se estará en presencia de un tratamiento engañoso o fraudulento o cuando:

I. Medie dolo, mala fe o negligencia en el tratamiento de datos personales que lleve a cabo;
II. Realice un tratamiento de datos personales que dé lugar a una discriminación injusta o arbitraria contra el titular, o
III. Vulnere la expectativa razonable de protección de datos personales.

Artículo 8.- Principio de Consentimiento. Cuando no se actualicen las causales de excepción previstas en la Ley, el servidor público responsable de recabar Datos Personales, deberá contar con el

consentimiento previo del titular para el tratamiento de los datos personales, el cual deberá otorgarse de forma:

I. Libre: sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular;

II. Específica: referida a finalidades concretas, lícitas, explícitas y legítimas que justifiquen el tratamiento; e

III. Informada: que el titular tenga conocimiento del aviso de privacidad previo al tratamiento a que serán sometidos sus datos personales.

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

Artículo 9.- Tipos de Consentimiento. El consentimiento podrá manifestarse de forma expresa o tácita.

El consentimiento es expreso cuando la voluntad del titular se manifieste verbalmente, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología. En el entorno digital, podrá utilizarse 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.

Para la obtención del consentimiento expreso, el responsable deberá facilitar al titular un medio sencillo y gratuito a través del cual pueda manifestar su voluntad.

Se entenderá que el titular consiente tácitamente el tratamiento de sus datos, cuando el aviso de privacidad es puesto a disposición y éste no manifiesta su voluntad en sentido contrario.

Tratándose de datos personales sensibles, se deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica o cualquier mecanismo de autenticación que al efecto se establezca, salvo en los casos previstos en esta Ley.

Será válido el consentimiento tácito, salvo que la Ley o las disposiciones aplicables exijan que la voluntad del titular se manifieste expresamente.

Artículo 10.-Principio de Calidad. El principio de calidad de los datos personales requiere que el servidor público adopte 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.

Se presume que se cumple con el principio de calidad en los datos personales cuando éstos 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 aplicables, deberán ser suprimidos, previo bloqueo en su caso y una vez que concluya el plazo de conservación de los mismos.

Artículo 11.- Principio de Proporcionalidad. Todo tratamiento de datos personales que efectúen los servidores públicos del IIEG, debe ser proporcional y solamente se podrán tratar datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron.

Capítulo II
Controles

Artículo 12.- Los directores de las áreas del IIEG, deberán notificar al Comité sobre el tipo de datos personales a los que da tratamiento, que se encuentren bajo su resguardo y responsabilidad; la cual podrá realizarse, ya sea por escrito o al correo oficial de la Unidad transparencia.iieg@jalisco.gob.mx .

En dicha notificación deberá precisar lo siguiente:

a. Tipos de datos personales que tengan en posesión, así como el personal a su cargo que tiene acceso a los mismos;
b. Tratamiento a los que son sometidos;
c. Si son sujetos de disociación;
d. Las bases de datos en las que se almacenan; su tipo de soporte, procesamiento, almacenamiento y organización; especificando en lo particular el personal que tiene acceso a cada una de éstas;
e. Tratamiento a los que son o serán sometidos;
f. Si son objeto de bloqueo y/o supresión.

Artículo 13.- Una vez notificada el Comité, el titular de la Unidad de Transparencia informará al Comité en su calidad de Secretario y éste último programará una sesión en la que deberá estar presente el Director del área responsable, con la finalidad que el Comité pueda determinar si es necesario se realice una Evaluación de Impacto en la Protección de Datos Personales; el tiempo de conservación, bloqueo y supresión de los mismos, dejando asentado en actas a los servidores públicos responsables que tengan acceso a las Bases de Datos.

Capítulo III
Acciones para restaurar la disponibilidad y el acceso a los datos personales, en caso de incidente físico o técnico.

Artículo 14.- En caso de sufrir un incidente físico o técnico que ponga en riesgo el tratamiento de los Datos Personales, o las Bases de Datos, se elaborará un documento por escrito, en el que consten las acciones de recuperación a emprender:

I. Continuidad de la Operación:
- a. Determinar si el sistema de tratamiento continúa con su operación después del incidente.
- b. En caso de que el sistema de tratamiento no continúe en operación después del incidente, se deberán indicar las causas.
- c. Informar sobre el personal designado para dar seguimiento a la recuperación del incidente, señalando el nombre completo y el puesto o cargo; siendo éste el equipo de respuesta a incidentes.

II. Tiempos:
- **a.** Fecha en que se detecta el incidente.
- **b.** Fecha en que fue atendido por el equipo de respuesta a incidentes.
- **c.** Fecha en que fue cerrado.
- **d.** Hora en que fue detectado.
- **e.** Hora en que fue atendido por el equipo de respuesta a incidentes.
- **f.** Hora en que fue cerrado.

III. Monitoreos:
- **a.** Describir las acciones que se realizarán para monitorear las medidas implementadas.
- **b.** Describir las herramientas para el monitoreo de las medidas implementadas (si es el caso).

IV. En la documentación del incidente, se deberá describir:
- **a.** Área involucrada.
- **b.** Sistema de tratamiento afectado.
- **c.** Información/datos personales involucrados en el incidente.
  - **i.** Resumen ejecutivo.
  - **ii.** Acciones realizadas.
  - **iii.** Impacto al sujeto obligado.
- **d.** Registros de comunicación sobre el incidente:
  - **i.** Fecha.
  - **ii.** Hora.
  - **iii.** Método (correo electrónico, teléfono, email, chat, etc)

iv. Nombre, tanto del iniciador, como del receptor.
v. Puesto y Área tanto del iniciador como del receptor.
vi. Organización o institución a la que pertenece.
vii. Información de contacto.
viii. Detalles de los hechos.

En el documento debe constar el nombre firma de quien realiza la recuperación y el nombre y firma de quien validó la recuperación.

Capítulo IV
Medidas correctivas y preventivas para la protección de los datos personales.

Artículo 15.- El director del área responsable, deberá elaborar un reporte final y completar la documentación de lo que se hizo respecto al incidente y comunicará al Comité el estado de seguridad de los datos personales después del incidente.

Artículo 16.- Para efectos de lo señalado en el artículo anterior, el Comité generará una bitácora con los reportes finales de incidentes, que permita a los encargados de dar respuesta a incidentes, contar con una base de conocimiento, que pueda ser utilizada para entrenar a los servidores públicos, así como a nuevos integrantes del equipo de respuesta a incidentes. Sin embargo, esta bitácora no estará a disposición de cualquier persona y solamente personal validado por el Comité tendrá acceso al mismo, y dicha bitácora será considerada como información reservada ya que de darse a conocer pone en riesgo las medidas de seguridad que se lleguen a implementar.

Artículo 17.- El reporte final de un incidente, deberá elaborarse en un tiempo no mayor a dos semanas después de erradicado el mismo, con la finalidad de perder detalles importantes sobre lo acontecido.