Políticas para la Protección de Datos Personales en el Municipio de Jocotepec, Jalisco

Índice

Políticas para la Protección de Datos Personales en el Municipio de Jocotepec, Jalisco

Naturaleza y aplicación:

La presentes Políticas son de orden público y de observancia general en el Municipio de Jocotepec, Jalisco, de conformidad con lo estipulado en los artículos 6 base A y 16, párrafo segundo de la Constitución Política de los Estados Unidos Mexicanos, así como del artículo 9°, de la Constitución Política del Estado de Jalisco, así como en el art. 29 numeral II de la Ley de Protección de Datos Personales en posesión de los sujetos obligados en el estado de Jalisco y sus Municipios.

Será aplicable a cualquier tratamiento de datos personales que obren en soportes físicos o electrónicos, con independencia del lugar, la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Objeto:

I. Establecer las bases, obligaciones, procedimientos y condiciones homogéneas que regirán el tratamiento de los datos personales y el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, mediante procedimientos sencillos y expeditos;

II. Garantizar la observancia de los principios de protección de datos personales previstos en la Ley General, Ley local y demás disposiciones aplicables;

III. Proteger los datos personales en posesión del Municipio de Jocotepec, Jalisco, con la finalidad de regular su debido tratamiento;

IV. Garantizar que toda persona pueda ejercer el derecho a la protección de los datos personales;

V. Promover, fomentar y difundir una cultura de protección de datos personales;

VI. Establecer los mecanismos para garantizar el cumplimiento y la efectiva aplicación de las medidas de apremio que correspondan para aquellas conductas que contravengan las disposiciones previstas en la Ley en materia;

VII. Regular el procedimiento y mecanismo necesario para la sustanciación del recurso de revisión a que se refiere la ley en materia;

VIII. Fijar los estándares y parámetros que permitan la implementación mantenimiento y actualización de medidas de seguridad de carácter administrativo, técnico, físico que permitan la protección de datos personales; y

IX. Establecer el catálogo de sanciones para aquellas conductas que contravengan las disposiciones previstas en la ley en materia.

Glosario:

I. Ajustes Razonables: Modificaciones y adaptaciones necesarias y adecuadas que no impongan una carga desproporcionada o indebida, cuando se requieran en un caso particular, para garantizar a las personas con discapacidad el goce o ejercicio, en igualdad de condiciones, de los derechos humanos;

II. Áreas: Instancias del Gobierno Municipal, 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;

III. 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;

IV. 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;

V. 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;

VI. Comité de Transparencia: Comité de Transparencia del Ayuntamiento de Jocotepec;

VII. Cómputo en la nube: Modelo de provisión externa de servicios de cómputo bajo demanda que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos digitales, en recursos compartidos dinámicamente;

VIII. Consentimiento: Manifestación de la voluntad libre, específica e informada del titular que autoriza el tratamiento de sus datos personales;

IX. 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;

X. 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;

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

XII. Días: Días hábiles;

XIII. 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;

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

XV. Encargado: Persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras, trata datos personales a nombre y por cuenta del responsable;

XVI. 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;

XVII. Fuentes de acceso público: Aquellas bases de datos, sistemas o archivos que por disposición de ley puedan ser consultados públicamente cuando no exista impedimento por una norma limitativa y sin más exigencia que, en su caso, el pago de una contraprestación, tarifa o contribución. No se considerará fuente de acceso público cuando la información contenida en la misma sea obtenida o tenga una procedencia ilícita, conforme a esta Ley y demás disposiciones aplicables;

XVIII. Instituto: Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco;

XIX. Instituto Nacional: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales;

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

XXI. Ley de Transparencia: Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios;

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

XXIII. Ley General de Transparencia: Ley General de Transparencia y Acceso a la Información Pública;

XXIV. 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;

XXV. 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;

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

XXVII. 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. De manera enunciativa más no limitativa, se debe 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 fuera de las instalaciones de la organización; y

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

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

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

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

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

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

XXIX. Plataforma Nacional: La Plataforma Nacional a la que hace referencia el artículo 49, de la Ley General de Transparencia;

XXX. Pleno del Instituto: Órgano máximo de gobierno del Instituto;

XXXI. Remisión: toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, con independencia de que se realice dentro o fuera del territorio mexicano;

XXXII. Responsable: Los sujetos obligados señalados en el artículo 1, párrafo 5, de la presente Ley que determinarán los fines, medios y alcance y demás cuestiones relacionadas con un tratamiento de datos personales.

XXXIII. Sistema Nacional: El Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales al que hace referencia la Ley General de Transparencia;

XXXIV. 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;

XXXV. Titular: Persona física a quien pertenecen los datos personales;

XXXVI. Transferencia: Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, responsable o encargado;

XXXVII. 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

XXXIII. Unidad de Transparencia: instancia que funge como vínculo entre el responsable y el titular, siendo la misma a la que se hace referencia en el artículo 31 de la Ley de Transparencia y en la Ley de Protección de Datos Personales.

Fuentes de acceso público.

1. Se considerarán como fuentes de acceso público:

I. Las páginas de Internet o medios remotos o locales de comunicación electrónica, óptica y de otra tecnología, siempre que el sitio donde se encuentren los datos personales esté concebido para facilitar información al público y esté abierto a la consulta general;

II. Los directorios telefónicos en términos de la normativa específica;

III. Los diarios, gacetas o boletines oficiales, de acuerdo con su normativa;

IV. Los medios de comunicación social; y

V. Los registros públicos conforme a las disposiciones que les resulten aplicables.

2. Para que los supuestos anteriores se consideren fuentes de acceso público será necesario que su consulta pueda ser realizada por cualquier persona no impedida por una norma limitativa, o sin más exigencia que, en su caso, el pago de una contraprestación, derecho o tarifa. No se considerará una fuente de acceso público cuando la información contenida en la misma sea o tenga una procedencia ilícita.

Límites y excepciones.

1. El Estado garantizará la privacidad de los individuos y velará porque terceras personas no incurran en conductas que puedan afectarla arbitrariamente.

2. No podrán tratarse datos personales sensibles, salvo que:

I. Los mismos sean estrictamente necesarios para el ejercicio y cumplimiento de las atribuciones y obligaciones expresamente previstas en las normas que regulan la actuación del responsable;

II. Se dé cumplimiento a un mandato legal;

III. Se cuente con el consentimiento expreso y por escrito del titular; o

IV. Sean necesarios por razones de seguridad pública, orden público, salud pública o salvaguarda de derechos de terceros.

3. En el tratamiento de datos personales de menores de edad se deberá privilegiar el interés superior de la niña, el niño y el adolescente, en términos de las disposiciones legales aplicables.

4. Los principios, deberes y derechos previstos en esta Ley y demás disposiciones aplicables tendrán como límite en cuanto a su observancia y ejercicio la protección de disposiciones de orden público, la seguridad pública, la salud pública o la protección de los derechos de terceros.

Interpretación.

1. En la aplicación e interpretación del presente se estará a lo dispuesto en la Constitución Política de los Estados Unidos Mexicanos, en los tratados internacionales de los que el Estado Mexicano sea parte, así como en las resoluciones, sentencias, determinaciones, decisiones, criterios y opiniones vinculantes, la Constitución Política del estado de Jalisco, entre otros, que emitan los

órganos internacionales especializados, privilegiando en todo momento la interpretación que más favorezca a los titulares.

2. Para el caso de la interpretación, se podrán tomar en cuenta los criterios, determinaciones y opiniones de los organismos nacionales e internacionales, en materia de protección de datos personales.

Principios y deberes

Principios

Observancia.

1. El responsable deberá observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información, y responsabilidad en el tratamiento de los datos personales.

Licitud.

1. 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.

Finalidad.

1. Todo tratamiento de datos personales que efectúe el responsable 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.

2. 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.

3. El responsable 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 esta Ley y demás disposiciones aplicables.

Lealtad.

1. El responsable no deberá obtener y tratar datos personales a través de medios engañosos o fraudulentos; deberá privilegiar la protección de los intereses del titular y la expectativa razonable de privacidad.

2. Se estará en presencia de un tratamiento engañoso o fraudulenta 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.

Consentimiento.

1. Cuando no se actualicen algunas de las causales de excepción previstas en presente Ley, el responsable deberá contar con el consentimiento previo del titular para el tratamiento de los datos personales, el cual deberá otorgarse de forma:

l. 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.

2. 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.

Tipos de Consentimiento.

1. 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.

2. 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.

3. 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.

4. Tratándose de datos personales sensibles, el responsable 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.

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

Excepciones al Principio de Consentimiento.

1. El responsable no estará obligado a recabar el consentimiento del titular para el tratamiento de sus datos personales en los siguientes casos:

I. Cuando una ley así lo disponga, debiendo dichos supuestos ser acordes con las bases, principios y disposiciones establecidos en esta Ley, en ningún caso, podrán contravenirla;

II. Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;

III. Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;

IV. Cuando los datos personales sean necesarios en la atención de algún servicio sanitario de prevención o diagnóstico;

V. Cuando los datos personales figuren en fuentes de acceso público;

VI. Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;

VII. Cuando los datos personales se sometan a un procedimiento previo de disociación;

VIII. Para el reconocimiento o defensa de derechos del titular ante autoridad competente;

IX. Cuando el titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley en la materia; o

X. Cuando las transferencias que se realicen entre responsables, sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales.

Calidad.

1. El principio de calidad de los datos personales requiere que el responsable 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.

2. 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.

3. 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.

Documentación de los procedimientos de conservación, bloqueo y supresión de los datos personales.

1. El responsable deberá establecer y documentar los procedimientos para la conservación, en su caso bloqueo y supresión de los datos personales en su posesión, en los cuales se incluyan los plazos de conservación de los mismos, conforme al artículo anterior.

2. En los procedimientos antes señalados el responsable deberá 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 su conservación.

Criterio de minimización.

1. El responsable procurará realizar esfuerzos razonables para tratar los datos personales al mínimo necesario, con relación a las finalidades que motivan su tratamiento.

Información.

1. El responsable deberá informar al titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.

2. 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.

3. El aviso de privacidad deberá ser difundido por los medios electrónicos y físicos con que se cuente, tales como medios impresos, sonoros, digitales, visuales o cualquier otra tecnología; con una redacción y estructura clara y sencilla, para cumplir con el propósito de informar.

4. Cuando resulte imposible dar a conocer al titular el aviso de privacidad de manera directa o ello exija esfuerzos desproporcionados, el responsable podrá instrumentar medidas compensatorias de comunicación masiva de acuerdo con los criterios que para tal efecto emita el Sistema Nacional.

5. El aviso de privacidad se redactará conforme a lo dispuesto en la Ley General.

6. En el caso de personas indígenas, el responsable hará los ajustes razonables pertinentes para dar a conocer el aviso de privacidad en su lengua de origen, con el objetivo de que el consentimiento sea considerado libre. Lo mismo aplicará para personas que comprendan el sistema braille y análogos.

Características del aviso de privacidad.

1. El aviso de privacidad deberá ser sencillo, con información necesaria, expresado en lenguaje claro y comprensible, y con una estructura y diseño que facilite su entendimiento. En el aviso de privacidad queda prohibido:

I. Usar frases inexactas, ambiguas o vagas;

II. Incluir textos o formatos que induzcan al titular a elegir una opción en específico;

III. Marcar previamente casillas, en caso de que éstas se incluyan para que el titular otorgue su consentimiento; y

IV. Remitir a textos o documentos que no estén disponibles para el titular.

Modalidades del aviso de privacidad.

1. El aviso de privacidad se pondrá a disposición del titular en tres modalidades: corto, simplificado e integral.

2. El aviso de privacidad corto se usará cuando el espacio utilizado para la obtención de los datos sea mínimo y limitado, de igual forma, los datos solicitados por el responsable deberán ser los básicos.

Información, aviso de privacidad corto.

1. El aviso corto deberá contener la siguiente información:

I. La identidad y domicilio del responsable;

II. Las finalidades del tratamiento; y

III. Los mecanismos que el responsable ofrece para que el titular conozca el aviso de privacidad integral.

Información, aviso de privacidad simplificado.

1. El aviso simplificado deberá contener la siguiente información:

I. La denominación del responsable;

II. Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquellas 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 de los tres órdenes de gobierno 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 que requieren el consentimiento del titular; y

V. El sitio donde se podrá consultar el aviso de privacidad integral.

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

3. Los mecanismos y medios a los que refiere la fracción IV de este artículo, 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.

Información, aviso de privacidad integral.

1. El aviso de privacidad integral, además de lo dispuesto en la fracción V del artículo anterior, deberá contener al menos, la siguiente información:

I. El domicilio del responsable;

II. Los datos personales que serán sometidos a tratamiento, identificando aquellos 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 aquellas que requieren el consentimiento del titular;

V. La información sobre el uso de mecanismos en medios remotos o locales de comunicación electrónica, óptica u otra tecnología, que permita recabar datos personales de manera automática y simultánea al tiempo que el titular hace contacto con los mismos, en su caso;

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

VII. El domicilio de la Unidad de Transparencia; y

VIII. Los medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad.

Momentos para la puesta a disposición del aviso de privacidad.

1. El responsable deberá poner a disposición del titular el aviso de privacidad simplificado en los siguientes momentos:

I. Cuando los datos personales se obtienen de manera directa del titular previo a la obtención de los mismos; y

II. Cuando los datos personales se obtienen de manera indirecta del titular previo al uso o aprovechamiento de éstos.

2. Las reglas anteriores no eximen al responsable de proporcionar al titular el aviso de privacidad integral en un momento posterior, conforme a las disposiciones aplicables de esta Ley.

Modificaciones al aviso de privacidad.

1. Cuando el responsable pretenda tratar los datos personales para una finalidad distinta, deberá poner a su disposición el aviso de privacidad con las características del nuevo tratamiento previo al aprovechamiento de los datos personales para la finalidad respectiva.

Instrumentación de medidas compensatorias.

1. Cuando resulte imposible dar a conocer al titular el aviso de privacidad de manera directa o ello exija esfuerzos desproporcionados, el responsable podrá instrumentar medidas compensatorias de comunicación masiva, de acuerdo con los criterios que para tal efecto emita el Sistema Nacional.

Responsabilidad.

1. El responsable deberá implementar los mecanismos necesarios para cumplir con los principios, deberes y obligaciones establecidos en esta Ley y rendir cuentas sobre el tratamiento de datos personales en su posesión al titular o al Instituto, según corresponda; observando la Constitución y los Tratados Internacionales en los que el Estado mexicano sea parte; en lo que no se contraponga con la normativa mexicana podrá valerse de estándares o mejores prácticas nacionales o internacionales para tales fines.

Mecanismos de Responsabilidad

1. Entre los mecanismos que deberá adoptar el responsable para cumplir con el principio de responsabilidad establecido en esta Ley están, al menos, los siguientes:

I. Destinar recursos autorizados para la instrumentación de programas y políticas de protección de datos personales;

II. Elaborar políticas y programas de protección de datos personales obligatorios y exigibles al interior de la organización del responsable;

III. Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales;

IV. Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran;

V. Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales;

VI. Establecer procedimientos para recibir y responder dudas y quejas de los titulares;

VII. Diseñar, desarrollar e implementar sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, conforme a esta Ley y demás disposiciones aplicables; y

VIII. Garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, cumplan con las obligaciones previstas en esta Ley y las demás aplicables.

Deberes

Seguridad de los datos personales.

1. Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico 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; sin perjuicio de lo establecido por las disposiciones vigentes en materia de seguridad emitidas por las autoridades competentes al sector que corresponda, cuando éstas contemplen una protección mayor para el titular o complementen lo dispuesto en esta Ley y demás disposiciones aplicables.

Medidas de seguridad.

1. Las medidas de seguridad adoptadas por el responsable deberán considerar:

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.

Acciones para el establecimiento y mantenimiento de medidas de seguridad.

1. Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes acciones interrelacionadas:

I. Crear políticas internas para la gestión y tratamiento de los datos personales, 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, uso y posterior supresión;

II. Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales;

III. Elaborar un inventario de datos personales y de los sistemas de tratamiento;

IV. Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal responsable, entre otros;

V. Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;

VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales;

VII. 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; y

VIII. Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

Contenido de las políticas internas de gestión y tratamiento de los datos.

1. Con relación a la fracción I del artículo anterior de la presente Ley, el responsable deberá incluir en el diseño e implementación de las políticas internas para la gestión y tratamiento de los datos personales, al menos, lo siguiente:

I. Los controles para garantizar que se valida la confidencialidad, integridad y disponibilidad de los datos personales;

II. Las acciones para restaurar la disponibilidad y el acceso a los datos personales de manera oportuna en caso de un incidente físico o técnico;

III. Las medidas correctivas en caso de identificar una vulneración o incidente en los tratamientos de datos personales;

IV. El proceso para evaluar periódicamente las políticas, procedimientos y planes de seguridad establecidos, a efecto de mantener su eficacia;

V. Los controles para garantizar que únicamente el personal autorizado podrá tener acceso a los datos personales para las finalidades concretas, lícitas, explícitas y legítimas que originaron su tratamiento, y

VI. Las medidas preventivas para proteger los datos personales contra su destrucción accidental o ilícita, su pérdida o alteración y el almacenamiento, tratamiento, acceso o transferencias no autorizadas o acciones que contravengan las disposiciones de esta Ley y demás aplicables.

Sistema de gestión y documento de seguridad.

1. Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión.

2. Se entenderá por sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, conforme a esta Ley y demás disposiciones aplicables.

Documento de seguridad.

1. El responsable deberá elaborar y aprobar un documento que contenga las medidas de seguridad de carácter físico, técnico y administrativo conforme a esta Ley y demás disposiciones aplicables.

2. El documento de seguridad será de observancia obligatoria para los encargados y demás personas que realizan algún tipo de tratamiento de datos personales.

Contenido del documento de seguridad.

1. El documento de seguridad deberá contener, al menos, lo siguiente:

I. El nombre de los sistemas de tratamiento o base de datos personales;

II. El nombre, cargo y adscripción del administrador de cada sistema de tratamiento y/o base de datos personales;

III. Las funciones y obligaciones de las personas que traten datos personales;

IV. El inventario de los datos personales tratados en cada sistema de tratamiento y/o base de datos personales;

V. La estructura y descripción de los sistemas de tratamiento y/o bases de datos personales, señalando el tipo de soporte y las características del lugar donde se resguardan;

VI. Los controles y mecanismos de seguridad para las transferencias que, en su caso, se efectúen;

VII. El resguardo de los soportes físicos y/o electrónicos de los datos personales;

VIII. Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales;

IX. El análisis de riesgos;

X. El análisis de brecha;

XI. La gestión de vulneraciones;

XII. Las medidas de seguridad físicas aplicadas a las instalaciones;

XIII. Los controles de identificación y autenticación de usuarios;

XIV. Los procedimientos de respaldo y recuperación de datos personales;

XV. El plan de contingencia;

XVI. Las técnicas utilizadas para la supresión y borrado seguro de los datos personales.

XVII. El plan de trabajo;

XVIII. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y

XIX. El programa general de capacitación.

Actualización del documento de seguridad.

1. El responsable deberá revisar el documento de seguridad de manera periódica, así como actualizar su contenido cuando ocurran los siguientes eventos:

I. Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;

II. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;

III. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida; y

IV. Se implementen acciones correctivas y preventivas ante una vulneración de seguridad ocurrida.

Vulneraciones de seguridad.

1. Se considerarán como vulneraciones de seguridad, en cualquier fase del tratamiento de datos personales, 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.

Bitácora de vulneraciones de seguridad ocurridas.

1. El responsable deberá llevar una bitácora de las vulneraciones a la seguridad ocurridas en la que se describa:

I. La fecha en la que ocurrió;

II. El motivo de la vulneración de seguridad; y

III. Las acciones correctivas implementadas de forma inmediata y definitiva.

Notificación de las vulneraciones de seguridad ocurridas.

1. El responsable deberá informar sin dilación alguna al titular y al Instituto las vulneraciones de seguridad ocurridas, que de forma significativa afecten los derechos patrimoniales o morales del titular, en un plazo máximo de setenta y dos horas en cuanto se confirmen y haya empezado a tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, a fin de que los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos.

Contenido de la notificación de la vulneración.

1. El responsable deberá informar al titular y al Instituto, al menos, lo siguiente:

I. La naturaleza del incidente;

II. Los datos personales comprometidos;

III. Las recomendaciones y medidas que el titular puede adoptar para proteger sus intereses;

IV. Las acciones correctivas realizadas de forma inmediata; y

V. Los medios donde puede obtener mayor información al respecto.

Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

1. En caso de que ocurra una vulneración a la seguridad de los datos personales, 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.

Acciones del Instituto derivadas de notificaciones de vulneraciones de seguridad.

1. Una vez recibida una notificación de vulneración por parte del responsable, el Instituto podrá realizar las investigaciones previas a que haya lugar con la finalidad de allegarse de elementos que le permitan, en su caso, iniciar un procedimiento de verificación en términos de lo dispuesto en esta Ley.

Deber de confidencialidad.

1. El responsable deberá 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 aún después de finalizar sus relaciones con el mismo; sin menoscabo de lo establecido en las disposiciones aplicables en materia de acceso a la información pública.