INFEJAL

POLÍTICAS INTERNAS DE SEGURIDAD Y PROTECCIÓN DE DATOS PERSONALES

CONTENIDO

Título Primero
DISPOSICIONES GENERALES

CAPÍTULO ÚNICO

Objeto y aplicación

Artículo 1. Las presentes políticas son de observancia obligatoria para el personal que labora y/o presta sus servicios en el Instituto de la Infraestructura Física Educativa del Estado de Jalisco, aplicables al tratamiento de datos personales que obren en soportes físicos y/o electrónicos con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización. Tienen por objeto desarrollar las disposiciones previstas en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios (LPDPSOEJ).

DEFINICIONES

Artículo 2. Además de las definiciones previstas en el artículo 3 de la Ley de protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, para los efectos de las presentes políticas se entenderá por:

LPDPSOEJ. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

INFEJAL. Instituto de la Infraestructura Física Educativa del Estado de Jalisco
Responsable. El Instituto de la Infraestructura Física Educativa del Estado de Jalisco, quien decide sobre el tratamiento de datos personales, de conformidad con el Artículo 1° de Ley General.

Titular.- Persona física a quien corresponden los datos personales.

Tratamiento.- 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.

Encargado. Persona física o jurídica pública perteneciente a la organización del responsable, que trate datos personales a nombre y por cuenta del responsable.

Supresión.- Baja archivística de los datos personales conforme a la normativa archivística aplicable; esto es, resultado de la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable.

Documento de Seguridad.- Instrumento que describe 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.

Remisión.-Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano.

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

Bases de Datos.- Conjunto ordenado de datos personales referentes a una persona física identificada o identificable. Fijados por criterios con independencia de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Bloqueo.- Identificación y conservación de datos personales una vez concluida la finalidad para la cual se recabaron, para determinar responsabilidades en relación con su tratamiento, hasta el plazo de su prescripción legal o contractual. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda.

Oficial de Datos Personales.- Persona con jerarquía o posición dentro del Instituto el cual formará parte de la Jefatura de Información Pública responsable de ejecutar las políticas transversales en materia de datos personales.

Título Segundo
PRINCIPIOS Y DEBERES

CAPÍTULO I
De los principios de protección de datos personales

Artículo 3. En todo tratamiento de datos personales, el responsable deberá observar los principios rectores de la protección de datos personales previstos en el título segundo capítulo primero, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

Solicitud de Consentimiento.

Artículo 4. En el caso que se requiera el consentimiento del titular para el tratamiento de sus datos personales, la solicitud del consentimiento deberá ser precisa y clara, estar redactada en un lenguaje accesible y sencillo.

Consentimiento tácito.

Artículo 5. El consentimiento será tácito cuando habiéndose puesto a disposición del titular el aviso de privacidad, éste no manifieste su voluntad en sentido contrario en términos de lo señalado en el artículo 14 de la LPDPSOEJ.

Cuando los datos no se recaben directamente del titular, éste tendrá un plazo de 3 días, contados a partir del día siguiente de recibir el aviso de privacidad por parte del responsable, quien deberá documentar la puesta a disposición del aviso, para que el titular, en su caso, manifieste su negativa al tratamiento de sus datos personales a través de escrito libre, que deberá presentar ante el INFEJAL.

En caso de que no manifieste su negativa en el plazo señalado en el párrafo anterior, se entenderá que ha entregado su consentimiento tácito para el tratamiento de sus datos personales.

Consentimiento expreso

Artículo 6. El consentimiento será expreso cuando la voluntad del titular se manifieste de forma verbal, por escrito, por medios electrónicos o cualquier otra tecnología en términos de lo señalado en

el artículo 14 de la LPDPSOEJ.

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 el cual le permita acreditar de manera indubitable y en su caso, documentar que el titular otorgó su consentimiento ya sea a través de una acción o una acción afirmativa clara.

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.

Obtención del consentimiento del titular cuando los datos personales se recaban directamente del titular

Artículo 7. El responsable deberá obtener el consentimiento del titular para el tratamiento de sus datos personales, en el mismo momento en que se soliciten, cuando se recaben directamente de este, 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.

Para efectos de las presentes políticas internas se entenderá que el responsable obtiene los datos personales directamente del titular cuando éste los proporciona a la persona que lo representa personalmente o por algún medio que permita su entrega directa como podrían ser medios electrónicos, ópticos, sonoros, visuales, vía telefónica, Internet o cualquier otra tecnología y/o medio.

Obtención del consentimiento del titular cuando los datos personales se recaben indirectamente de éste

Artículo 8. Cuando el responsable recabe datos personales indirectamente del titular y se requiera de su consentimiento conforme a lo previsto en el artículo 14 de la LPDPSOEJ, éste no podrá tratar los datos personales hasta que cuente con la manifestación de la voluntad libre, específica e informada del titular, mediante la cual autoriza el tratamiento de los mismos ya sea de manera tácita o expresa, según corresponda.

Para efectos de las presentes políticas internas se entenderá que el responsable obtiene los datos personales indirectamente del titular cuando no han sido proporcionados en los términos a que se refiere el artículo anterior, segundo párrafo.

Revocación del consentimiento

Artículo 9. En cualquier momento, el titular, podrá revocar el consentimiento que ha otorgado para el tratamiento de sus datos personales sin que se atribuyan efectos retroactivos a la revocación, a través del ejercicio de los derechos de cancelación y oposición de conformidad con lo dispuesto por la LPDPSOEJ.

Presunción de calidad de los datos personales cuando se obtienen indirectamente del titular

Artículo 10. Cuando los datos personales fueron obtenidos indirectamente del titular, el responsable deberá optar medidas de cualquier naturaleza dirigidas a garantizar que estos responden al principio de calidad, de acuerdo con la categoría de datos personales y las condiciones y medios del tratamiento.

Principio de Información

Artículo 11. El responsable deberá informar a los titulares, a través del aviso de privacidad, la existencia y las características principales del tratamiento al que serán sometidos sus datos personales.

Medios de difusión del aviso de privacidad

Artículo 12. El responsable podrá difundir, poner a disposición o reproducir el aviso de privacidad en formatos físicos y electrónicos, ópticos, sonoros, visuales o a través de cualquier otra tecnología que permita su eficaz comunicación.

El aviso de privacidad se difundirá en el portal oficial de internet del Instituto, así como en las unidades administrativas internas en las que de acuerdo a sus funciones y obligaciones recaben de manera directa o indirecta datos personales, de conformidad con el Inventario de Datos personales, contenido en el Documento de Seguridad.

Momentos para la puesta a disposición del aviso de privacidad simplificado e integral

Artículo 13. El responsable a través de los encargados deberá poner a disposición del titular el aviso de privacidad simplificado en un primer momento. Lo cual no le impide que pueda dar a conocer el aviso de privacidad integral desde un inicio si o prefiere.

En ambos casos, el aviso de privacidad se pondrá conforme a las siguientes reglas:

> **I.** De manera previa a la obtención de los datos personales, cuando los mismos se obtengan directamente del titular, independientemente de los formatos o medios físicos y/o electrónicos utilizados para tal fin, o
>
> **II.** Al primer contacto con el titular o previo al aprovechamiento de los datos personales, cuando éstos se hubieren obtenido de manera indirecta del titular.

Una vez puesto a disposición del titular el aviso de privacidad simplificado conforme a lo dispuesto en el párrafo anterior del presente artículo; el aviso de privacidad integral deberá estar publicado, de manera permanente, en el sitio o medio que se informe en el aviso de privacidad simplificado, a efecto de que el titular lo consulte en cualquier momento.

Casos en los que se requiere un nuevo aviso de privacidad

Artículo 14. El responsable deberá poner a disposición del titular, un nuevo aviso de privacidad, en sus dos modalidades, de conformidad

con lo que establece la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios y las presentes políticas cuando:

I. Cambie su identidad

II. Requiera recabar datos personales sensibles adicionales a aquéllos informados en el aviso de privacidad original, los cuales no se obtengan de manera directa del titular y se requiera de su consentimiento para el tratamiento de éstos;

III. Cambie las finalidades señaladas en el aviso de privacidad original, o

IV. Modifique las condiciones de las transferencias de datos personales o se pretendan realizar transferencias no previstas inicialmente y el consentimiento del titular sea necesario.

En cualquiera de los supuestos señalados con antelación la unidad administrativa que trata datos personales deberá solicitar a la Unidad de Transparencia, mediante oficio la modificación y/o creación de un nuevo aviso de privacidad, justificando la finalidad y los cambios necesarios para el tratamiento de datos.

La Unidad de Transparencia deberá someter la propuesta del nuevo aviso de privacidad al Comité de Transparencia para su validación.

Artículo 15. El responsable no podrá llevar a cabo tratamiento de datos personales que tengan como efecto la discriminación de los titulares por su origen étnico o racial, su estado de salud presente, pasado o futuro, su información genética, sus opiniones políticas, su religión o creencias filosóficas o morales y su preferencia sexual, con especial énfasis en aquellos automatizados.

CAPÍTULO II
De los encargados, funciones y obligaciones

Artículo 16. Es responsabilidad de los encargados que en el ejercicio de sus funciones obtenga, use registre, organice, conserve, elabore, utilice, comunique, difunda, almacene, posea, maneje, aproveche,

divulgue, transfiera o disponga de datos personales, observar los principios rectores de la protección de datos personales, previstos en el título segundo capítulo primero de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

Funciones y Obligaciones

Artículo 17. Para efectos de estas políticas Internas, se entenderá como encargado, el responsable que en términos del artículo anterior, trate

datos personales, mismos que se detallan en el inventario de datos personales contenido en el Documento de Seguridad.

Artículo 18. El encargado, deberá observar al momento de recabar datos personales lo siguiente:
I. Dar un uso a los datos personales respetando la ley, desde el momento de su obtención.

II. No utilizar medios engañosos o fraudulentos para obtener los datos personales.

III. Poner a disposición el aviso de privacidad, de tal manera que el titular pueda conocer de qué forma serán tratados sus datos personales y cómo podrá ejercer sus derechos ARCO.

IV. Obtener el consentimiento o autorización del titular para el tratamiento de sus datos personales, salvo las excepciones previstas en el artículo 70 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como el artículo 15 y 75 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

V. Cuando se recaben datos personales sensibles, el consentimiento del titular deberá ser expreso y por escrito. En el caso de datos personales de carácter patrimonial o financiero, el consentimiento del titular deberá ser expreso únicamente. Fuera de estos dos casos, como regla general es válido el

consentimiento tácito (principio de consentimiento) siempre y cuando se ponga a disposición de los individuos titulares de los datos, el aviso de privacidad, en el que se indique lo que se hará con su información.

VI. Evitar la creación de bases de datos de carácter sensible, salvo que se justifique plenamente la necesidad del tratamiento para la consecución de finalidades legítimas y concretas relacionadas con las actividades estatutarias o comerciales que persigue el responsable.

VII. Recabar sólo aquellos datos personales que sean necesarios para las finalidades para las que se obtienen.

Artículo 19. El encargado, deberá observar durante el manejo y/o utilización de los datos personales lo siguiente:
I. Utilizar los datos personales respetando la Ley.

II. Respetar la expectativa razonable de privacidad del titular, es decir, la confianza que depositó este último en el responsable, respecto de los datos personales que serán tratados conforme a lo que acordaron y en los términos establecidos por la Ley.

III. Limitar el tratamiento de la información personal al cumplimiento de las finalidades previamente consentidas por el titular.

IV. Usar los datos personales que resulten estrictamente necesarios para cumplir con las finalidades para las cuales fueron recabados.

V. Mantener los datos personales actualizados y correctos.

VI. Limitar el periodo de conservación de la información personal tratada al mínimo necesario.

VII. Mantener la confidencialidad de los datos personales tratados.

VIII. Implementar medidas de seguridad de carácter administrativo, físico y técnico que garanticen la confidencialidad e integridad de los datos personales.

IX. Informar al titular, sin demora alguna, sobre las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de éste, en cuanto se confirme la vulneración sucedida.

X. Adoptar las medidas necesarias para cumplir con las obligaciones establecidas en la Ley.

XI. Rendir cuentas al titular en caso de algún incumplimiento con relación a la protección de sus datos personales.

Designación del oficial de protección de datos personales

Artículo 20. El instituto como responsable que en ejercicio de sus funciones sustantivas lleven a cabo tratamientos relevantes o intensivos de datos personales, podrá designar un oficial de protección de datos personales, el cual formará parte de la Unidad de Transparencia.

La persona designada como oficial de protección de datos deberá contar con jerarquía dentro del Instituto que le permita implementar políticas transversales en esta materia. El oficial de protección de datos personales será designado por el Comité de transparencia atendiendo a sus conocimientos, cualidades profesionales, experiencia en la materia y, en su caso a la o las certificaciones con que cuente en materia de protección de datos personales.

Funciones del oficial de protección de datos personales
Artículo. 21. El oficial de protección de datos personales tendrá las siguientes atribuciones:

I. Asesorar al Comité de Transparencia respecto a los temas que sean sometidos a su consideración en materia de protección de datos personales

II. Proponer al Comité de Transparencia políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la Ley General y la ley estatal en materia de protección de datos personales

III. Dar seguimiento a las políticas, acciones, y demás actividades que correspondan para el cumplimiento a las determinaciones que en materia de datos personales haya aprobado el

Comité de Transparencia.

IV. Realizar los monitoreos con la periodicidad que determinen las presentes políticas, así como los que para el caso concreto determine el Comité de transparencia.

V. Proponer al Comité de Transparencia en coordinación con el Órgano Interno de Control del Instituto el plan de Auditoría interna.

VI. Asesorar permanente a las áreas pertenecientes al Instituto en materia de protección de datos personales, y

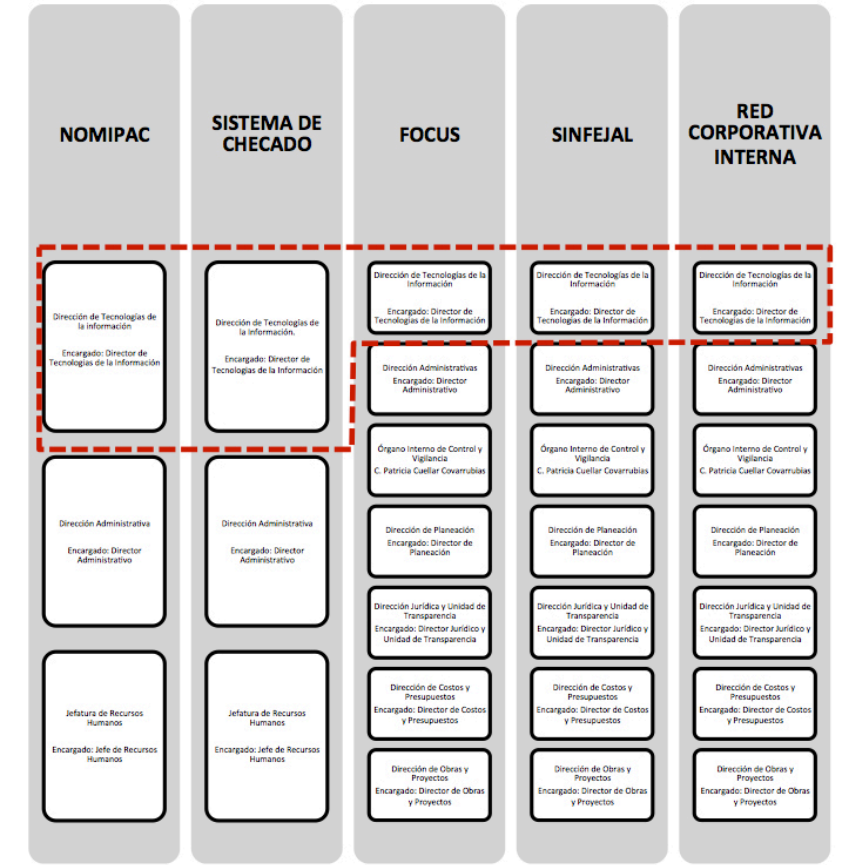
VII. Las demás que determine el responsable y la normatividad que resulte aplicable.

Título Tercero
SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

CAPÍTULO ÚNICO
De los Sistemas y los Encargados

Artículo 22. De acuerdo con el Sistema de Gestión de Seguridad de los Datos Personales, y el documento de Seguridad del Instituto, se identifican los siguientes sistemas electrónicos del Instituto.

Dentro del diagrama se resalta con una línea punteada de color tinto, a la Dirección encargada de resguardar la seguridad de los sistemas electrónicos del Instituto, mientras que los que están fuera de la línea punteada son también administradores pero éstos se encargan de los resguardos físicos mientras que los que están fuera de la línea punteada son también administradores pero éstos se encargan de los resguardos físicos.



Artículo 23. Son objeto de tratamiento los datos personales de servidores públicos, personas físicas y personas morales.

El acopio de los datos personales de los servidores públicos y de personas físicas que laboren y/o presten un servicio en el instituto, tiene por objeto integrar el expediente laboral, a fin de realizar los trámites administrativos, fiscales y jurídicos correspondientes.

Por su parte, la recolección de datos de personas morales tiene como finalidad la realización de trámites y servicios administrativos de conformidad con las atribuciones conferidas a este organismo público descentralizado debiendo ser adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.

Artículo 24. Entre los datos personales sometidos a tratamiento se encuentran: nombre, domicilio, teléfono, registro federal de contribuyentes, clave única de registro de población, número de cuenta, correo electrónico, capital social, datos de asamblea de accionistas, folio mercantil de registro público de la propiedad y comercio, registro patronal, número de cédula profesional e imagen del personal que ingresa a laborar, los cuales se detallan en el Inventario de Datos Personales.

Título cuarto.
DEL CICLO DE VIDA DE LOS DATOS PERSONALES

CAPÍTULO I
Conservación y Utilización de los Datos

Artículo 25. Una vez que el encargado recolecta los datos personales, realizará su tratamiento de acuerdo a su finalidad, conservando los datos y/o documentos en los espacios que para el fin se destinen observando las medidas de seguridad física, administrativas y técnicas que se establecen en el Documento de Seguridad.

Artículo 26. Tratándose de documentos que contengan datos personales, su conservación obedecerá a lo establecido en el catálogo de disposición documental, de acuerdo a su sección, sub sección y serie.

Artículo 27. Tratándose de datos introducidos a bases de datos en cumplimiento a la finalidad de su recolección, su resguardo será electrónico en el servidor del Instituto observando las medidas de seguridad física, administrativas y técnicas que se establecen en el Documento de Seguridad.

Artículo 28. El Inventario de datos personales y el sistema de tratamiento de los mismos se describen en el documento de Seguridad del Instituto, integrándose por cada base de datos una cedula de identificación.

Supresión de Datos Personales

Artículo 29. En la supresión de datos personales que 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, atendiendo a las técnicas para la supresión y borrado seguro para los datos personales establecidas en el Documento de Seguridad.

CAPÍTULO II
Transferencia de Datos Personales

Artículo 30. Para informar al titular sobre las transferencias nacionales y/o internacionales de datos personales que en su caso efectúe el responsable y que no requieran del consentimiento del titular, el Instituto deberá indicar en el aviso de privacidad integral lo siguiente;

I. Los destinatarios o terceros receptores, de carácter público o privado, nacional y/o internacional, de los datos personales; identificando cada uno de estos por su nombre, denominación o razón social;

II. Las finalidades de las transferencias de los datos personales relacionadas por cada destinatario o tercero receptor, y

III. El fundamento legal que lo faculta o autoriza para llevarlas a cabo, señalando el o los artículos, apartados, fracciones, incisos y nombre de los ordenamientos o disposición normativa vigente, precisando su fecha de publicación o, en su caso, la fecha de la última reforma o modificación.

Artículo 31. Cuando la transferencia de datos personales requiera el consentimiento expreso del titular, el responsable podrá establecer cualquier medio que le permita obtener esta modalidad del consentimiento de manera previa a la transferencia de sus datos personales, siempre y cuando el medio habilitado sea de fácil acceso y con la mayor cobertura posible, considerando el perfil de los titulares y la forma en que mantienen contacto cotidiano a común con el titular.

Transferencias nacionales de Datos Personales

Artículo 32. Cuando la transferencia sea nacional, el receptor de los datos personales asumirá el carácter de responsable conforme a la legislación que en esta materia le resulte aplicable atendiendo su naturaleza jurídica, pública o privada, y deberá tratar los datos personales atendiendo a dicha legislación y a lo convenido en el aviso de privacidad que le será comunicado por el responsable transferente.

Transferencia internacional de datos personales

Artículo 33. El responsable sólo podrá transferir datos personales fuera del territorio nacional, cuando el receptor o destinatario se obligue a proteger los datos personales conforme a los principios, deberes y demás obligaciones similares o equiparables a las previstas en la Ley General y demás normatividad mexicana en la materia, así como a los términos previstos en el aviso de privacidad que le será comunicado por el responsable transferente.

Artículo 34.-La formalización de las transferencias de datos personales se realizará mediante acuerdo en el cual deberá asentarse lo siguiente:

I.Área responsable que realiza la transferencia de datos personales, y fundamento legar interno que le otorga facultades y atribuciones

II. Datos personales objeto de tratamiento de acuerdo al aviso de Privacidad Integral

III. Fundamento de la transferencia de datos personales

IV. Supuesto de excepción al consentimiento respecto de la transferencia y/o consentimiento del titular sobre la transferencia de datos personales

V. Finalidad de la Transferencia

VI. Responsabilidades del destinatario o terceros receptores de datos personales

VII. Lugar, fecha y hora de la transferencia

VIII. Firma del responsable que transfiere y firma del responsable que recibe.

Artículo 35.-Las comunicaciones de datos personales que se realicen entre el responsable y encargado se llaman remisiones; no requieren ser informadas al titular, ni contar con su consentimiento.

Artículo 36.- Las remisiones que se realicen entre encargados, deberán formalizarse mediante acuerdo de Remisión de Datos Personales, cual deberá asentarse lo siguiente:

I. Área responsable que realiza la transferencia de datos personales, y fundamento legar interno que le otorga facultades y atribuciones

II. Datos personales objeto de tratamiento de acuerdo al aviso de Privacidad Integral

III. Fundamento de la transferencia de datos personales

IV. Supuesto de excepción al consentimiento respecto de la transferencia y/o consentimiento del titular sobre la transferencia de datos personales

V. Finalidad de la Transferencia

VI. Responsabilidades del destinatario o terceros receptores de datos personales

VII. Lugar, fecha y hora de la transferencia

VIII. Firma del responsable que transfiere y firma del responsable que recibe.

Artículo 37. La carga de la prueba para acreditar el cumplimiento de las obligaciones previstas en el presente título, recaerá en todo momento, en el responsable.

Título Quinto.
DE LA SUPERVISIÓN PERIÓDICA Y VULNERACIONES DE SEGURIDAD

CAPÍTULO I
Del monitoreo y evaluación de resultados

Artículo 38. Para la evaluación de resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales a fin de verificar el cumplimiento de los objetivos planteados, el comité de Transparencia a través del oficial de datos personales monitoreará anualmente lo siguiente:

I. Los nuevos activos que se incluyan en la gestión de riesgos

II. Las modificaciones necesarias a los activos, como podrán ser el cambio o migración tecnológica, entre otras:

III. Las nuevas amenazas que podrían estar activas dentro y fuera del Instituto y que no han sido valoradas

IV. La posibilidad de vulneraciones nuevas o incrementadas sean explotadas por las amenazas correspondientes,

V. Las vulnerabilidades identificadas para determinar aquellas expuestas a amenazas nuevas o pasadas que vuelvan a surgir,

VI. El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y

VII. Los incidentes y vulneraciones de seguridad ocurridos.

Artículo 39. El monitoreo y revisión de las medidas de seguridad se realizarán anualmente observando lo previsto en el Documento de Seguridad y en su caso lo que establezca el Comité de Transparencia, quien deberá establecen en sesión ordinaria el periodo de evaluación así como la metodología a utilizar.

Artículo 40.- Se realizará de manera anual la revisión del Plan de Seguridad de Datos Personales el cual abordará por lo menos lo siguiente:

• Revisión del Documento de Seguridad en el que deben recogerse los procedimientos, medidas de seguridad y controles necesarios para una adecuada protección de los datos personales (automatizados o no) y el estricto cumplimiento de la Ley y legislación complementaria.

• El Documento de Seguridad se completará con las políticas internas actualizadas que en materia de Protección de datos y seguridad de la información se encuentran implantadas en el Instituto.

• Revisión y en su caso, redacción de anexos al Documento de Seguridad y en particular:

o Cédula de bases de Datos Personales

o Bitácoras de acceso y operación cotidiana

o Bitácoras de vulneración de seguridad de los datos personales

o Registro de encargados de seguridad de datos personales

CAPÍTULO II
Notificaciones de vulneraciones de seguridad

Artículo 41. El responsable deberá notificar al Comité de Transparencia así como al oficial de protección de datos personales, las vulneraciones de seguridad que de forma significativa afecten los derechos patrimoniales o morales del titular dentro del plazo máximo de setenta y dos horas, a partir de que confirme la ocurrencia de estas y el responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de mitigación de la afectación.

Artículo 42. Para efectos del artículo anterior se entenderá que se afectan los derechos patrimoniales del titular cuando la vulneración esté relacionada, de manera enunciativa más no limitativa, con sus bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados o las cantidades o porcentajes relacionados con la situación económica del titular.

Se entenderá que afectan los derechos morales del titular cuando la vulneración esté relacionada, de manera enunciativa más no limitativa, con sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, configuración y aspectos físicos, consideración que de sí mismo tienen los demás, o cuando se menoscabe ilegiblemente la libertad o la integridad física o psíquica de éste.

Notificación de las vulneraciones al Órgano Garante

Artículo 43. En términos de lo previsto en el artículo 40 de la ley en materia de protección de datos en el estado, el responsable deberá informar mediante escrito presentado en el domicilio del Órgano garante del estado, o bien, en cualquier otro medio que se habilite para tal efecto, al menos, lo siguiente:

I. La hora y la fecha de la identificación de la vulneración

II. La hora y la fecha del inicio de la investigación sobre la vulneración

III. La naturaleza del incidente o vulneración ocurrida

IV. La descripción detallada de las circunstancias en torno a la vulneración ocurrida

V. Las categorías y números aproximados de titulares afectados

VI. Los sistemas de tratamiento y datos personales comprometidos

VII. Las acciones correctivas realizadas de forma inmediata

VIII. La descripción de las posibles consecuencias de la vulneración de seguridad ocurrida

IX. Las recomendaciones dirigidas al titular

X. El medio puesto a disposición del titular para que pueda obtener mayor información al respecto

XI. El nombre completo de la o las personas designadas y sus datos de contacto, para que puedan proporcionar mayor información al órgano garante

XII. Cualquier otra información y documentación que considere conveniente hacer del conocimiento del órgano garante.

Notificación de las vulneraciones de seguridad al Titular

Artículo 44. En la notificación que realice el responsable al titular sobre las vulneraciones de seguridad a que se refiere el artículo el artículo 40 de la LPDPSOEJ, deberá informar al titular de los datos personales, al menos lo siguiente:

I. La naturaleza del incidente o vulneración ocurrida

II. Los datos personales comprometidos

III. Las recomendaciones dirigidas al titular sobre las medidas que éste pueda adoptar para proteger sus intereses

IV. Las acciones correctivas realizadas de forma inmediata

V. Los medios puestos a disposición del titular para que pueda obtener mayor información al respecto,

VI. La descripción de las circunstancias generales en torno a las vulneración ocurrida, que ayuden al titular a entender

el impacto del incidente y,

VII. Cualquier otra información y documentación que considere conveniente para apoyar a los titulares.

El responsable deberá notificar directamente al titular la información a la que se refieren las fracciones anteriores a través de los medios que establezca para tal fin.

CAPÍTULO III

Auditorías Internas

Artículo 45. El oficial de protección de datos personales en coordinación con el Órgano Interno de Control y Vigilancia presentará ante el Comité de Transparencia el programa de auditoría.

Artículo 46.- La auditoría consistirá en las siguientes etapas:

I.Análisis y revisión detallados de la situación actual sobre el cumplimiento y adecuación a la normativa:

- Identificación de bases de datos y sus niveles de seguridad
- Identificación de usuarios que tratan las Bases de Datos
- Identificación del flujo de datos
- Identificación de terceros con acceso a datos (encargados de tratamiento)
- Identificación de posibles cesiones de datos
- Revisión de los sistemas de información (redes, servidores, instalaciones, centros de trabajo, software de tratamiento de datos personales)

II. Informe de diagnóstico y recomendaciones

A**rtículo 47.** Las auditorías referidas en el artículo anterior se realizarán por el Órgano Interno de Control y Vigilancia, quien establecerá las etapas y periodicidad para su realización.

Transitorios

Primero. Las presentes políticas entrarán en vigor 10 días hábiles siguiente de la aprobación por parte del Comité de Transparencia.

Segundo. Se establece un periodo de 10 días hábiles posteriores a la aprobación de las presentes políticas para su difusión y capacitación al personal del Instituto, cuya responsabilidad estará a cargo de la Jefatura de Información Pública.

infejal.jalisco.gob.mx

 @INFEJAL  Infejal

AV. PROLONGACIÓN ALCALDE # 1350,
Col., Miraflores, Guadalajara, Jalisco, México.
Tels: 01 (33) 3819 5220, 3824 9952.