## REQUISITOS DEL CONTENIDO DEL SISTEMA DE GESTIÓN DE DATOS PERSONALES

| Requisitos | Consideraciones |
|---|---|
| **Fase Planear** | |
| **1. Contar con alcances y objetivos definidos. (Parámetro 17)** | De acuerdo con los Parámetros, el alcance de un esquema debe considerar principios, deberes y obligaciones, de la siguiente manera:<br><br>**Un alcance total considera todos los principios, deberes y obligaciones establecidos en la normativa:**<br>**Principios:**<br>• Principio de licitud.<br>• Principio de consentimiento.<br>• Principio de información.<br>• Principio de calidad.<br>• Principio de finalidad.<br>• Principio de lealtad.<br>• Principio de proporcionalidad.<br>• Principio de responsabilidad.<br>**Deberes:**<br>• Seguridad.<br>• Confidencialidad.<br>**Obligaciones:**<br>• Vinculadas a la relación entre encargado y responsable.<br>• Vinculadas con la transferencia de datos personales.<br>• Vinculadas con la atención de solicitudes de derechos ARCO de los titulares.<br><br>**Un alcance parcial considera uno o algunos de los principios, deberes y obligaciones señaladas anteriormente.** |
| **2. Contar con una Política de Gestión de Datos Personales, que sea comunicada a todos los miembros que participen con el responsable o encargado, la Política deberá describir al menos: (Parámetro 18)** | Además, es relevante que la Política de Gestión de Datos Personales esté aprobada (firmada) por un miembro de la alta dirección, quien puede ser la persona asignada para la implementación y desarrollo del SGDP (numeral 19 y 20 de los Parámetros).<br><br>La política debe establecer el compromiso de cumplir con las leyes vigentes en términos de protección de datos personales, por lo que debe ser comunicada a toda la organización. |
| 2.1 Los tratamientos a que aplica (Numeral 18, fracción I, de los Parámetros) | El tratamiento de datos puede entenderse como cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados realizadas sobre datos personales, relacionadas, de manera enunciativa más no limitativa, con la obtención, acceso, registro, organización, estructuración, adaptación, indexación, modificación, extracción, consulta, almacenamiento, conservación, elaboración, transferencia, difusión, posesión, aprovechamiento y en general cualquier uso o disposición de datos personales. |

| | |
|---|---|
| | En este apartado se deben definir los tratamientos relacionados con el ámbito personal de aplicación, es decir, con el grupo de titulares cuyos datos personales están vinculados con el tratamiento al que aplica el esquema (fracción v, numeral 14 de los Parámetros),<br><br>Para el caso de tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla al menos con lo establecido en el Artículo 52 del Reglamento en sus fracciones I y II. |
| 2.2 Acciones a realizar para el cumplimiento del principio, deber u obligación a que se enfoca (Numeral 18, fracción II, de los Parámetros); | En la Política se deberán describir de manera general las acciones que se llevarán a cabo para dar cumplimiento de cada uno de los principios, deberes y obligaciones, considerando el alcance del esquema, ya sea total o parcial.<br><br>Para lo anterior, se podrá apoyar de la "Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares"[1], en la cual se encuentran algunas acciones recomendadas. |
| 2.3 Acciones para el desarrollo, implementación, mantenimiento y mejora continua del SGDP (Numeral 18, fracción III, de los Parámetros), y | Se deberán describir en este apartado las acciones que definen las tareas para desarrollar, implementar, mantener la implementación y actualizar el SGDP, esto como un compromiso de mejora continua del sistema de gestión de datos personales. |
| 2.4 Las buenas prácticas que decidan adoptar, en su caso (Numeral 18, fracción III, de los Parámetros). | La organización podrá integrar buenas prácticas, a fin de complementar o facilitar el cumplimiento de lo dispuesto por la Ley, su Reglamento y demás disposiciones aplicables, con objeto de abordar situaciones o problemáticas particulares, que no hayan sido previstas en el carácter general de la normativa.<br><br>Las buenas prácticas integradas en el esquema serán obligatorias para quien esta adherido al esquema, por lo que deberán identificarse en los procedimientos, acciones y/o actividades en las que se integren a lo largo del esquema. |
| **3. Participación de la Alta Dirección (Numerales 4, fracción II, 19 y 20 de los Parámetros):** | |
| 3.1 El apoyo a la Política para garantizar el compromiso del responsable con el SGDP. | A través de la Política, la alta dirección define un marco de referencia para que se comunique lo que se pretende lograr en cuanto a la protección de datos personales durante el desarrollo, implementación, mantenimiento y mejora continua del SGDP.<br><br>Para demostrar el apoyo de la alta dirección se puede evidenciar lo siguiente:<br><br>a) Presentar la política sea aprobada (firmada) por la alta dirección y compartida con los integrantes de la organización. (Parámetro 18);<br>b) Presentar una exposición y explicación detallada del COMPROMISO con el esquema de autorregulación. Documento debidamente firmado por el miembro de la alta dirección,<br>c) Determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGDP. (Parámetro 22) |

[1] Disponible en: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Guia_obligaciones_lfpdppp_junio2016.pdf

| | |
|---|---|
| | En caso de que se trate de un grupo de empresas adheridas, se deberá adjuntar la Política firmada e información requerida por cada alta dirección de cada organización, o en su defecto, señalar que se trata de la misma alta dirección si así fuera el caso. |
| 3.2 La designación de uno de sus miembros para la realización de:<br><br>• Planeación, implementación y desarrollo del SGDP;<br>• Coordinación de la elaboración del SGDP y de la Política;<br>• Las gestiones necesarias para la aprobación del SGDP y de la Política por parte de la Alta Dirección, y<br>• Las acciones necesarias para asegurar la implementación y cumplimiento del SGDP y de la Política | El responsable o encargado deberá designar a un miembro de la alta dirección para planear, implementar y desarrollar el SGDP.<br>Entre las responsabilidades de esta persona estarán, al menos las establecidas en las fracciones I, II y III del numeral 20 de los Parámetros.<br><br>En caso de que se trate de un grupo de empresas adheridas, se deberán evidenciar las designaciones de cada miembro de la alta dirección en cada organización, o bien, detallar en caso de que se trate de la misma alta dirección señalarlo. |
| **4. Designación de personal (permanentes y temporales, proveedores externos, consultores y/o asesores) que esté a cargo del cumplimiento cotidiano del SGDP y de la Política con la responsabilidad: (Parámetro 21)** | El responsable o encargado deberá designar al personal que considere necesario para estar a cargo del cumplimiento cotidiano del SGDP y de la Política de Gestión de Datos Personales.<br><br>La designación del personal que estará cargo del cumplimiento cotidiano del SGDP y de la política de gestión de datos personales, deberá presentarse firmada, pero además deberá contener como mínimo las responsabilidades establecidas en las 10 fracciones del numeral 21 de los Parámetros.<br><br>En caso de que sea más de una persona encargada, pueden ser divididas o compartidas las responsabilidades establecidas en los Parámetros, a discreción de la organización.<br><br>Para cuando se trate de un grupo de empresas adheridas, se deberá evidenciar esta designación por cada organización, a menos de que sea el mismo personal designado para estar a cargo del cumplimiento cotidiano del SGDP para todas las empresas adheridas, lo cual deberá estar indicado. |

| | |
|---|---|
| **5. Determinar y asignar recursos materiales, financieros y humanos necesarios para establecer, implementar, operar, mantener y mejorar el SGDP.**<br>**(Parámetro 22)** | La Alta Dirección debe establecer el compromiso de la asignación de recursos materiales, financieros y humanos necesarios para establecer, implementar, operar, mantener y mejorar el SGDP.<br><br>Este apartado está relacionado con el Parámetro 19, es relevante que la asignación de recursos sea clara y precisa.<br><br>Cuando se trate de un grupo de empresas que están adheridas al mismo esquema, deberán presentar la asignación de recursos de manera individual, o bien, establecer de manera clara que la asignación descrita incluye a todas las empresas adheridas. |
| **Fase Hacer** | |
| **6. Fomentar una cultura de protección de datos personales a través de:**<br><br>**(Parámetro 23)** | Los responsables y/o encargados deberán considerar realizar programas de capacitación y programas de sensibilización al interior de la organización, así como, generar mecanismos que se emplearán para medir la eficacia de los programas. Además, deberán de comunicar a todo el personal la importancia de alcanzar los objetivos del SGDP y el cumplimiento de la política, asimismo, deberán asegurarse de que todos sus miembros están sensibilizados sobre la contribución del cumplimiento de objetivos y las consecuencias de las no conformidades. Finalmente deberán prever mecanismos para reportar asuntos relevantes a los miembros de la alta dirección. |
| 6.1. Capacitación continua y programas de sensibilización con relación a la protección de los datos personales y el SGDP; | Se deberá presentar un documento en el que se identifiquen tanto el programa de capacitación como el de sensibilización relacionados con temas en materia de protección de datos personales. Lo anterior, debe ser documentado desde su planeación hasta su aplicación.<br><br>Cabe señalar, que los programas de capacitación continua guardan relación con el cumplimiento de la normativa en materia de protección de datos personales y la operación del SGDP, mientras que los programas de sensibilización deberán guardar relación con la concientización sobre la importancia del adecuado tratamiento de los datos personales y las posibles consecuencias del incumplimiento, entre otros. |
| 6.2. Establecimiento de un proceso para la evaluación de la efectividad de la capacitación y los programas de sensibilización; | En este apartado, se deberá presentar el documento en el que conste el proceso en que el responsable o encargado realizará la evaluación de la efectividad de la capacitación y de los programas de sensibilización.<br><br>Considerando que un proceso es una secuencia de acciones ejecutadas, para evaluar en este caso, la efectividad. Por lo que, podrán integrarse los criterios que considerarán para la evaluación.<br><br>Lo anterior, debe ser documentado desde su planeación hasta su aplicación. |
| 6.3 Comunicación a todo el personal sobre la importancia de:<br><br>- Alcanzar los objetivos del SGPD,<br>- Cumplir con la Política, y<br>- Actualizar la Política y el SGDP; | El responsable y/o encargado deberá establecer:<br><br>• Cómo va a comunicarse con el personal, es decir, el medio de difusión que será utilizado.<br>• El contenido de la comunicación.<br>• Cada cuanto se hará la comunicación.<br><br>Considerando lo anterior, además de comunicar la Política, se deberá comunicar al personal la importancia de alcanzar los objetivos establecidos en el sistema de gestión de datos personales, la importancia de cumplir con la Política y de actualizar la política y el SGDP. todo ello planificar y documentarse. Lo anterior, debe ser documentado desde su planeación hasta su aplicación. |

| | |
|---|---|
| | Algunos ejemplos de forma de comunicación pueden ser correos electrónicos, plataformas, fondos de pantalla, entre otros. |
| 6.4. Aseguramiento de que todos sus miembros estén sensibilizados de su contribución para alcanzar los objetivos del SGPD y las consecuencias de las no conformidades, y | Además de realizar sensibilización en materia de protección de datos personales, como se establece en el punto 6.1, el responsable y encargado deberá sensibilizar a todos los miembros en específico de la contribución de cada uno de ellos para alcanzar los objetivos fijados por la empresa para cumplir con el sistema de gestión de datos personales, así mismo, sensibilizar sobre las posibles consecuencias de que al no cumplir con lo establecido en el sistema de gestión de datos personales, se generen no conformidades y cuál sería el impacto. Lo anterior, debe ser documentado desde su planeación hasta su aplicación. |
| 6.5. Previsión de mecanismos de reporte de asuntos relevantes a los niveles superiores. | El responsable o encargado, deberá establecer un mecanismo -técnica o herramienta que permita llevar a cabo de manera pertinente, efectiva y adecuada la acción de realizar los reportes- que considere apropiado para generar el reporte de los asuntos relevantes en materia del fomento de la cultura de la protección de datos personales a la alta dirección, en el cual se informe de los puntos anteriores. Esto deberá ser documentado desde su planeación hasta su aplicación. |
| **7. Elaborar y mantener actualizado, un inventario de los datos personales con lo siguiente: (Parámetro 24)** | |
| 7.1. El listado de datos que trate, o de sus categorías, y | El responsable y/o encargado, deberá documentar en el inventario de datos personales los datos personales tratados, o las categorías de los mismos.<br><br>Los datos personales son cualquier información concerniente a una persona física identificada o identificable, como puede ser el nombre, los apellidos, la dirección postal, el número de teléfono, la dirección de correo electrónico, el número de pasaporte, una fotografía, la Clave Única de Registro de Población (CURP) o cualquier otra información que permita identificar o haga identificable al titular de los datos.<br><br>Los datos personales pueden estar expresados en forma numérica, alfabética, gráfica, fotográfica, acústica o en cualquier otra modalidad.<br><br>Es importante que en el inventario se integren todos los datos personales (o sus categorías), que son TRATADOS por la organización considerando el ámbito personal de aplicación que está determinado como parte del alcance del esquema.<br><br>En caso de que se trate de un grupo de empresas adheridas, se deberá integrar el inventario de cada una de ellas, considerando que, se pudieran tener diferentes áreas que tratan los datos personales o quizá diferentes datos personales que son tratados en cada una de las empresas adheridas. |
| 7.2. Las finalidades de su tratamiento. | El responsable y/o encargado, deberá incluir en el inventario de datos personales las finalidades del tratamiento.<br><br>Los datos personales sólo pueden ser tratados para cumplir con la finalidad o finalidades que hayan sido informadas al titular en el aviso de privacidad y, en su caso, consentidas por éste. Se debe entender por finalidad del tratamiento, el propósito, motivo o razón por el cual se tratan los datos personales.<br><br>Las finalidades deben ser licitas del tratamiento de datos personales, es decir, deberán especificar para qué objeto se tratarán los datos personales de manera clara, sin lugar a confusión y con objetividad. En este sentido, se deberán evitar finalidades inexactas, |

| | |
|---|---|
| | ambiguas o vagas, como “de manera enunciativa más no limitativa”, “entre otras finalidades”, “por ejemplo”, entre otros.<br><br>En el caso de que se consideren finalidades secundarias, también deberán formar parte del inventario.<br><br>Es relevante que se pueda evidenciar la relación de las finalidades con cada dato personal tratado, y que esto sea congruente con los avisos de privacidad. |
| **8. Documentar el flujo de los datos personales dentro del responsable incluyendo**: **(Parámetro 24)** | |
| 8.1. La obtención, uso, divulgación, transferencias, almacenamiento, bloqueo y cancelación. | Una vez que se ha realizado el inventario de datos personales, la siguiente acción consiste en identificar el flujo de los datos personales, al interior de la organización.<br><br>El responsable y/o encargado deberá documentar e integrar como parte del inventario, el flujo de los datos personales, es decir, la trazabilidad de los datos personales dentro de la organización, considerado el tratamiento de los datos que se realicen desde su obtención, uso, divulgación, transferencias, almacenamiento, bloqueo, cancelación, supresión o destrucción.<br><br>En este sentido, para la elaboración del flujo de datos se deberá considerar al menos lo siguiente:<br><br>1. El flujo de los datos personales dentro de la organización (obtención, uso, divulgación, transferencias, almacenamiento, bloqueo, cancelación, supresión o destrucción).<br>2. Identificar las áreas de la organización que utilizan los datos personales en las distintas fases del tratamiento. |
| **9. Realizar un análisis de riesgo. (Parámetro 25)** | |
| 9.1 Implementación de un procedimiento para Identificar riesgos; | El responsable y/o encargado, deberá desarrollar un procedimiento para identificar riesgos.<br><br>Para la identificación de riesgos, se sugiere considerar lo siguiente:<br>a) Identificación de activos y sistemas de tratamiento (**Artículo 61, fracción I del RLFPDPPP**). Para la identificación de activos se puede considerar lo siguiente:<br><br>- **Activos de información**, corresponden a la esencia de la organización[2]:<br>• Información relativa a los datos personales, y<br>• Información de procesos en los que interviene el flujo de datos personales y actividades involucradas en el tratamiento de los mismos.<br><br>- **Activos de apoyo**, en los cuales residen los activos de información, como son:<br>• Hardware;<br>• Software;<br>• Redes y Telecomunicaciones;<br>• Personal;<br>• Estructura organizacional, e infraestructura adicional.<br><br>En este sentido, al identificar en que activos y sistemas de tratamiento se encuentran los datos personales, es posible identificar los riesgos de esos activos. |

[2] Disponible para su consulta en: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf

| | |
|---|---|
| 9.2. Implementación de un procedimiento para evaluar el grado de riesgo asociado a cada tratamiento de datos personales que realiza por sí mismo o a través de un encargado, y | El responsable y/o encargado, deberá realizar una evaluación del grado de riesgo asociado a cada tratamiento de datos personales, de manera libre podrán elegir la metodología para la evaluación de riesgos que considere adecuada.<br><br>El objetivo de este apartado es que los responsables y/o encargados determinen el impacto que el riesgo pueda tener sobre los datos personales que tratan, con el fin de que prioricen y tomen la mejor decisión respecto a los controles más relevantes e inmediatos a implementar.<br><br>Para evaluar el grado de riesgo de cada dato personal, así como en su conjunto, se debe considera el apartado 9.1, que es la identificación de los riesgos.<br><br>Para elaboración del procedimiento del análisis del riesgo, deberá considerarse el punto anterior 9.1, así como lo establecido en el a través de la elaboración de un análisis de riesgos (**Artículo 61 fracción III del RLFPDPPP**), el cual consiste en identificar peligros y estimar los riesgos de los datos personales.<br>**Artículo 60, fracción I, III y IX del RLFPDPPP** |
| 9.3. Gestionar los riesgos identificados para mitigar la posibilidad de cualquier vulneración a los datos personales. | La gestión de riesgos deberá guardar relación con la Política de Gestión de Datos Personales, con la finalidad de dar cumplimiento a las metas y compromisos establecidos en el SGDP.<br><br>Una vez realizado el análisis de riesgos establecido en el punto 9.2, se deberán gestionar los riesgos identificados.<br><br>Para ello, independientemente de la metodología que será utilizada y documentada, se deberá considerar lo establecido en el **RLFPDPPP, en los Artículos 60, 61 fracciones II, IV, V, VI, VII, VIII, IX, 62,64, 65 y 66.**<br><br>En este sentido, de manera general se deberá realizar un análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquellas faltantes que resulten necesarias para la protección de los datos personales, para ello, podrá elegirse la metodología que decida la organización, determinar medidas de seguridad aplicables a los datos personales que se traten, determinar un plan de trabajo para implementar las medidas de seguridad faltantes y llevar a cabo revisiones o auditorias. |
| **10. Capacitación especializada. (Parámetro 26)** | |
| 10.1. Asegurar que el personal designado para estar a cargo del cumplimiento cotidiano del SGDP y la política Tenga competencia en el conocimiento de la Ley, su Reglamento y demás normativa y buenas prácticas aplicables; | El personal asignado para estar a cargo del cumplimiento cotidiano del SGDP y la Política, que fue designado de acuerdo con lo establecido en el Parámetro 21, deberá contar con documentación que demuestre las competencias de conocimiento de la LFPDPPP y demás normativa aplicable, por ejemplo, considerar temas enfocados a la introducción de la Ley, cumplimiento a los principios, deberes y obligaciones, entre otros. |
| 10.2. Asegurar que el personal designado para estar a cargo del cumplimiento | El personal asignado para estar a cargo del cumplimiento cotidiano del SGDP y la Política, además, deberá mantenerse informado y actualizado sobre cuestiones relacionadas con el tratamiento de datos personales, por lo que, deberá documentar y evidenciarlo en el esquema. |

| | |
|---|---|
| cotidiano del SGDP y la política se mantenga informado y actualizado sobre cuestiones relacionadas con el tratamiento de datos personales; | |
| 10.3. Asegurar que el personal designado para estar a cargo del cumplimiento cotidiano del SGDP y la política entienda sus funciones y responsabilidades para que los datos personales sean tratados de conformidad con los procedimientos preestablecidos, y | El personal asignado para estar a cargo del cumplimiento cotidiano del SGDP y la Política deberá entender sus funciones y responsabilidades, para que los datos sean tratados de conformidad con los procedimientos establecidos en todo el SGDP, para ello, se recomienda desarrollar un procedimiento y criterios que permitan evaluar que el personal, efectivamente entiende sus funciones y responsabilidades.<br><br>Las funciones y obligaciones mínimas que deberá atender y comprender el personal a cargo del cumplimiento cotidiano del SGDP y la Política están descritas en el Parámetro 21. |
| 10.4. Asegurar que el personal designado para estar a cargo del cumplimiento cotidiano del SGDP y la política reciba la capacitación que resulte necesaria para la debida realización de sus funciones. | El personal asignado para estar a cargo del cumplimiento cotidiano del SGDP y la Política deberá recibir capacitación continua, planeada y programada, que resulte necesaria para un mejor desempeño de sus funciones.<br><br>En este sentido, por ejemplo, si unas de las funciones y responsabilidades son "vigilar la implementación del SGDP, realizar auditorías, coordinar tareas de gestión de riesgo y aspectos de seguridad" entonces, en el programa de capacitación especializada se integrarán temas como:<br><br>▪ Sistema de Gestión de Datos Personales o en su caso, en lo relativo a la familia ISO 27000;<br>▪ Gestión de riesgos,<br>▪ Auditorías;<br>▪ Entre otros.<br><br>Es importante que se documente lo relativo a la capacitación, desde su planeación hasta su ejecución. |
| **Fase Hacer** | |
| **11. Desarrollar e implementar procedimientos específicos en materia de datos personales. (Parámetro 27)** | |
| 11.1 Desarrollo e implementación de procedimientos específicos para el tratamiento de datos personales bajo todos los principios previstos en la Ley y su Reglamento cuando se trate de un esquema total o, | El responsable y/o encargado, deberá considerar el alcance descrito en los numerales 1 (alcance y objetivos) y 2 (Política de SGDP), y deberá establecer un procedimiento para evidenciar el cumplimiento de cada uno de los principios que atiende el esquema de autorregulación. En caso, de que su esquema no integre en su alcance algún principio, deberá omitir atender este punto, ya que no le es aplicable.<br><br>En este orden de ideas, lo que se debe describir e integrar en este aparado son reglas, pautas y/o instrucciones precisas sobre cómo deben ejecutarse los procedimientos dentro de la organización para dar cumplimiento a cada principio, según sea el caso. |

| | |
|---|---|
| en caso de tratarse de un esquema parcial, el que sea aplicable; | En el caso de incluir buenas prácticas, estás deberán guardar congruencia con lo descrito en el numeral 2.4 (Buenas prácticas).<br><br>Se sugiere tomar como referencia la Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, disponible en:<br>https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Guia_obligaciones_lfpdppp_junio2016.pdf |
| 11.2. El tratamiento de datos personales bajo los deberes previstos en la Ley y su Reglamento cuando se trate de un esquema total o, en caso de tratarse de un esquema parcial, el que sea aplicable; | El responsable y/o encargado, deberá considerar el alcance descrito en los numerales 1 (alcance y objetivos) y 2 (Política de SGDP), y deberá establecer un procedimiento para evidenciar el cumplimiento de cada uno de los deberes que atiende el esquema de autorregulación. En caso, de que su esquema no integre en su alcance algún deber, deberá omitir atender este punto, ya que no le es aplicable.<br><br>En este orden de ideas, lo que se debe describir e integrar en este aparado son las reglas, pautas y/o instrucciones precisas sobre cómo deben ejecutarse los procedimientos dentro de la organización cumplir con cada deber, según sea el caso.<br><br>En el caso de incluir buenas prácticas, estás deberán guardar congruencia con lo descrito en el numeral 2.4 (Buenas prácticas).<br><br>Se sugiere tomar como referencia la Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, disponible en:<br>https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Guia_obligaciones_lfpdppp_junio2016.pdf |
| 11.3 El cumplimiento de las obligaciones en materia de protección de datos personales previstas por la Ley, su Reglamento, cuando se trate de un esquema total o, en caso de tratarse de un esquema parcial, el que sea aplicable; | El responsable y/o encargado, deberá considerar el alcance descrito en los numerales 1 (alcance y objetivos) y 2 (Política de SGDP), y deberá establecer un procedimiento para evidenciar el cumplimiento de cada una de las obligaciones que atiende el esquema de autorregulación. En caso, de que su esquema no integre en su alcance alguna obligación, deberá omitir atender este punto, ya que no le es aplicable.<br><br>En este orden de ideas, lo que se debe describir e integrar en este aparado son las reglas, pautas y/o instrucciones precisas sobre cómo deben ejecutarse los procedimientos dentro de la organización para dar cumplimiento a cada obligación, según sea el caso.<br><br>En el caso de incluir buenas prácticas, estás deberán guardar congruencia con lo descrito en el numeral 2.4 (Buenas prácticas).<br><br>Se sugiere tomar como referencia la Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, disponible en:<br>https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Guia_obligaciones_lfpdppp_junio2016.pdf |
| 11.4. La atención de los derechos de ARCO, así como la revocación del consentimiento, de conformidad con lo previsto por la Ley, | El derecho a la protección de datos personales es un derecho personal, solamente los titulares o sus representantes podrán solicitar el ejercicio de los derechos ARCO.<br><br>En ese sentido, cuando el esquema sea total o bien, parcial e incluya esta obligación, la organización deberá desarrollar un procedimiento que evidencie la atención que dará cuando un titular solicite algún derecho ARCO, así como un procedimiento para la revocación del consentimiento. |

| | |
|---|---|
| su reglamento y demás normativa y buenas prácticas aplicables cuando se trate de un esquema total, o en caso de tratarse de un esquema parcial, sólo cuando éste trate sobre la atención de los derechos ARCO; | En este orden de ideas, lo que se debe describir e integrar son las reglas, pautas y/o instrucciones precisas sobre cómo deben ejecutarse los procedimientos dentro de la organización para dar cumplimiento a esta obligación.<br><br>En el caso de incluir buenas prácticas, estás deberán guardar congruencia con lo descrito en el numeral 2.4 (Buenas prácticas).<br><br>Se sugiere tomar como referencia la Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, disponible en:<br>https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Guia_obligaciones_lfpdppp_junio2016.pdf |
| 11.5. La atención a quejas relacionadas con el tratamiento de datos personales; | En términos del Artículo 14 de la Ley Federal, el responsable o encargado, deberá adoptar medidas para garantizar el tratamiento, privilegiando el interés del titular. Es por ello, que deberá establecer procedimientos para recibir, responder dudas y quejas de los titulares de los datos personales.<br><br>Es decir, que deberá establecer y documentar las acciones específicas para la atención a quejas relacionadas con el tratamiento de datos personales, además de identificar al personal que esté a cargo de dar seguimiento de este punto y definir el plazo para su atención.<br><br>En el caso de incluir buenas prácticas, estás deberán guardar congruencia con lo descrito en el numeral 2.4 (Buenas prácticas). |
| 11.6. La transferencia de datos personales de conformidad con lo previsto por la Ley, su Reglamento y demás normativa y buenas prácticas aplicables cuando se trate de un esquema total, o en caso de tratarse de un esquema parcial, sólo cuando éste trate sobre transferencias; | Una transferencia de datos personales se debe entender como toda comunicación de datos realizada a persona distinta del responsable o encargado del tratamiento[3].<br><br>Cuando el esquema sea total o bien, parcial que integre en el alcance transferencias de datos personales, deberá incorporar al esquema los procedimientos documentados que llevará a cabo la organización, así mismo deberá señalar si las transferencias son nacionales, internacionales, si requieren consentimiento, o no y a quien se transfieren.<br><br>Para lo anterior, el responsable o encargado deberá considerar lo establecido en el capítulo V de la Ley Federal, capítulo IV del RLFPDPPP, y demás disposiciones aplicables.<br><br>En el caso de incluir buenas prácticas, estás deberán guardar congruencia con lo descrito en el numeral 2.4 (Buenas prácticas).<br><br>Se sugiere tomar como referencia la Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, disponible en:<br>https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Guia_obligaciones_lfpdppp_junio2016.pdf |
| 11.7. La regulación de la relación con los encargados, cuando éstos estén presentes en el esquema, de | El encargado es la persona física o moral, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras, trata datos personales por cuenta del responsable, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio. |

[3] Definición obtenida de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

| | |
|---|---|
| conformidad con lo previsto por la Ley, su Reglamentos y demás normativa y buenas prácticas aplicables cuando se trate de un esquema total, o en caso de tratarse de un esquema parcial, sólo cuando éste trate sobre la relación con los encargados; | Cuando el esquema sea total, o bien, parcial que integre en el alcance la regulación de la relación con los encargados, se deberá incorporar al esquema los procedimientos que realice o vaya a realizar la empresa para cumplir con la regulación con los encargados. Lo anterior, de conformidad con lo establecido en la Ley Federal, su Reglamento y demás normativa.<br><br>De conformidad con el artículo 50 del Reglamento de la Ley Federal, el responsable deberá contemplar ciertas obligaciones del encargado en el instrumento jurídico en el que establezca la relación jurídica con éste. Además, deberá considerar lo establecido en el artículo 52 del Reglamento de la Ley Federal, cuando se trate de contrataciones de servicio de cómputo en la nube.<br><br>En el caso de incluir buenas prácticas, estás deberán guardar congruencia con lo descrito en el numeral 2.4 (Buenas prácticas).<br><br>Se sugiere tomar como referencia la Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, disponible en:<br>https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Guia_obligaciones_lfpdppp_junio2016.pdf |
| 11.8. El adecuado tratamiento de datos personales de categorías especiales de titulares, tales como menores de edad, personas adultas mayores, personas con discapacidad, migrantes, y | En caso de que los tratamientos contemplen las categorías especiales de titulares, tales como menores de edad, personas adultas mayores, personas con discapacidad, migrantes, deberá documentar los procedimientos específicos para cada caso de las categorías especiales.<br><br>En el caso de incluir buenas prácticas, estás deberán guardar congruencia con lo descrito en el numeral 2.4 (Buenas prácticas). |
| 11.9. El desarrollo, implementación, mantenimiento y mejora continua del SGDP. | El responsable y/o encargado deberá integrar en el esquema los procedimientos que va a seguir o sigue para desarrollar, implementar, mantener y realizar una mejora continua del SGDP.<br><br>Dicho lo anterior, se deberá incorporar al esquema los procedimientos, acciones, criterios, específicos y claros de los procedimientos que se llevarán a cabo para cada fase del SGDP. |
| **12. Actualización del SGDP (Parámetro 28)** | |
| 12.1 Revisar y evaluar el SGDP y la Política | El responsable y/o encargado deberá programar las revisiones de rutina que realice el personal referido en el Parámetro 21 quien está a cargo de operar el SGDP y la Política, así como establecer un formato de evaluación para que pueda documentar la evaluación realizada para verificar si se da cumplimiento a los objetivos planteados con respecto a la Ley y demás normativa en materia.<br><br>En caso de que se detecte que no se ha dado cumplimiento, deberán documentar en el formato establecido para ello, las modificaciones y actualizaciones al SGDP y Política que resulten necesarios, esto puede generarse entre otros motivos por algún cambio en la propia normativa en materia, cambio de tecnología o cualquier otra situación que resulte relevante. |
| **13. Planear, implementar y mantener un programa de auditoría. (Parámetros 29, 30 y 31)** | |

| | |
|---|---|
| 13.1 Planeación, implementación y mantenimiento de un programa de auditoría que incluya el objeto de monitorear y revisar la conformidad de los tratamientos de datos personales realizados por el responsable, incluidos aquéllos efectuados por sus encargados, con relación a la Política | El responsable y/o encargado deberá identificar en el programa de auditorías el objeto del monitoreo con la finalidad de que se tengan identificadas las acciones a realizar de los auditores en la organización, tomando en consideración los tratamientos y el cumplimiento de la política.<br><br>Los auditores puedes ser internos o externos. |
| 13.2. Planeación, implementación y mantenimiento de un programa de auditoría que incluya el aseguramiento de la objetividad e imparcialidad de las auditorías a través de una adecuada selección de auditores y la debida realización de éstas; | El responsable y/o encargado deberá seleccionar a los auditores previamente, para ello, tendrá que definir si el auditor será interno o externo.<br><br>Para asegurar la objetividad e imparcialidad de las auditorías a través de una adecuada selección de auditores, la organización deberá establecer mecanismos, criterios o procedimientos que deberá documentar en el esquema.<br><br>Existen diversos supuestos que se sugiere considerar en este punto:<br><br>a) Cuando el auditor forme parte de la organización, deberá existir independencia en la toma de decisiones, la entrega de resultados al personal correspondiente para la atención de los resultados correspondientes a las auditorías. Deberá documentar las actividades, funciones y obligaciones del o de los auditores en el Sistema de Gestión. Así mismo el auditor o equipo auditor deberá contar con evidencia de la formación correspondiente de manera enunciativa más no limitativa en temas como auditoría en 27001, sistema de gestión de datos personales, así como de la normativa en materia de datos personales. Es decir, deben demostrar la competencia en lo que van a auditar, en ese sentido, tendría que ser en el sistema de gestión de datos personales.<br>b) En el caso de que el auditor o auditores sean externos a la organización, será relevante documentar la información que demuestre su competencia en materia de auditoría, en sistema de gestión de datos personales, en protección de datos personales, es decir, que sea competente en el tema auditado. |
| 13.3. Planeación para su realización en intervalos de al menos un año para determinar si el SGDP está operando, se implementa y se mantiene de conformidad con la Política, requerimientos y procedimientos establecidos; | El responsable y/o encargado deberá establecer un programa de auditoría que incluya la frecuencia.<br><br>En este sentido, se deberá incluir la calendarización de auditorías en intervalos de al menos un año, para determinar si el SGDP se encuentra operando de conformidad con lo planteado en la fase de Planeación del esquema. |

| | |
|---|---|
| 13.4. Presentación de reportes que detallen cualquier no conformidad con la Política que incluyan:<br>- Cifras, indicadores y estadísticas relacionadas con los procedimientos puestos en operación,<br>- Recomendaciones necesarias a fin de hacer más efectivo y eficiente el cumplimiento de la Política y el SGDP.<br>- La identificación de asuntos relacionados con la tecnología o procesos que pudieran afectar el cumplimiento de la Política. | El responsable y/o encargado deberá desarrollar formatos para documentar los reportes que detallen las no conformidades con la Política, con la finalidad de informar a la alta dirección sobre los resultados de las auditorías, estos formatos de reportes deben incluir como mínimo:<br><br>a. Cifras, indicadores y estadísticas relacionadas con los procedimientos puestos en operación, que permitan identificar el cumplimiento de la política, requerimientos y procedimientos establecidos. Dichos indicadores permitirán conocer el cumplimiento del objetivo, así como la oportunidad de mejora en el ciclo de vida del SGDP.<br>b. Recomendaciones necesarias a fin de hacer más efectivo y eficiente el cumplimiento de la Política y el SGDP.<br>c. La identificación de asuntos relacionados con la tecnología o procesos que pudieran afectar el cumplimiento de la Política. |
| **14. Planear, implementar y mantener revisión administrativa. (Parámetro 32)** | |
| 14.1 Previsión, implementación y mantenimiento de revisiones administrativas regulares y programadas. | El responsable y/o encargado deberá realizar una programación de las revisiones administrativas, estas revisiones deben de ser regulares con el fin de asegurar la conveniencia, adecuación y eficacia continua del SGDP. |
| 14.2. Que las revisiones administrativas tengan por objeto asegurar un adecuado desarrollo continuo y la efectividad del SGDP. | El responsable y/o encargado deberá incluir en la programación de las revisiones administrativas cuál es el objeto de esas revisiones, con la finalidad de asegurar un adecuado desarrollo continuo y sobre todo, la efectividad del SGDP de conformidad con la normativa aplicable y el objetivo del propio SGDP |
| 14.3. Previstas cuando se lleven a cabo cambios que afecten aspectos significativos del SGDP como:<br>·En la normativa aplicable,<br>·En la tecnología, o | El responsable y/o encargado deberá documentar un procedimiento para realizar una revisión administrativa cuando se realice un cambio en el SGDP que afecte su funcionamiento, como puede ser una actualización de la normativa aplicable, o bien, un cambio en la tecnología implementada en los procesos de la organización, un cambio de los valores y/o procedimientos que integran el SGDP.<br><br>Toda revisión administrativa debe ser documentada. |

| | |
|---|---|
| ·En los valores y procedimientos del responsable. | |
| 14.4. Basadas en:<br>· La retroalimentación por parte de los usuarios del SGDP;<br>· Los riesgos identificados en el análisis de riesgos;<br>· Los resultados de auditorías;<br>· Los resultados de las revisiones;<br>· Las actualizaciones o cambios en la tecnología utilizada por el responsable;<br>· Los requerimientos por parte de autoridades;<br>· El manejo de quejas, y<br>· Las vulneraciones de seguridad. | Al realizar una revisión administrativa, se deben considerar al menos lo contenido en el Parámetro 32 fracciones de la I a la VIII. En este sentido, el responsable y/o encargado deberá contar con un procedimiento y/o formato para realizar las revisiones administrativas, en el cual se considere como mínimo:<br>1. La retroalimentación por parte de los usuarios del SGDP, es decir, de quien está operando el SGDP<br>2. Los riesgos identificados en el análisis de riesgos; es decir, los resultados de la evaluación de riesgos y el estado del plan de tratamiento de los riesgos. Relacionado con el punto 9 (Análisis de riesgos) de los requisitos del SGDP del presente documento.<br>3. Los resultados de auditorías; es decir, los estados de las acciones de auditorías anteriores. Relacionado con el punto 12 (Auditorías).<br>4. Los resultados de las revisiones; es decir, los estados de las acciones de anteriores revisiones administrativas, cuando para la presentación del esquema se hayan aplicado previamente otras revisiones administrativas.<br>5. Las actualizaciones o cambios en la tecnología utilizada por el responsable; cuando se haya actualizado o cambiado la tecnología utilizada en el SGDP.<br>6. Los requerimientos por parte de autoridades<br>7. El manejo de quejas, es decir, la información considerada en el punto 11.5 (Atención a quejas).<br>8. Las vulneraciones de seguridad, que se hayan generado y documentado en el punto 9 (Análisis de riesgos). |
| 14.5. Estar documentadas. | El responsable y/o encargado deberá documentar lo señalado en todo el apartado 13, ya sean formatos o procedimientos y en su caso, evidencias correspondientes. |
| 14.6. Ser realizadas por el personal previamente asignado. | Es relevante que se designe al personal que lleve a cabo las revisiones administrativas, lo anterior, se sugiere realizar a través de un oficio de designación debidamente firmado. |
| Fase Actuar | |
| **15. Aplicar acciones preventivas y correctivas (Parámetros 33, 34 y 35)** | |
| 15.1. Para la Implementación de acciones preventivas para evitar cualquier no conformidad, se debe considerar:<br>I. Determinar e implementar dichas acciones según sean requeridas;<br>II. Conservar los resultados y las revisiones de las acciones implementadas; | I. El responsable y/o encargado deberá establecer criterios para identificar cuándo se determina una acción preventiva, además desarrollar procedimientos para implementar las acciones preventivas con la finalidad de mejorar el SGDP.<br>De igual forma, es relevante asignar al personal encargado de darle seguimiento a las mismas.<br>II. El responsable y/o encargado deberá establecer los plazos para conservar los resultados y las revisiones de las acciones implementadas.<br>Asimismo, deberá establecer los medios de eliminación seguros de dicha información al concluir el plazo de conservación.<br>III. El responsable y/o encargado deberá identificar aquellos casos en los que una no conformidad requiera acciones correctivas en lugar de acciones preventivas |

| | |
|---|---|
| III. Identificar posibilidades de cambio que pudieren dar lugar a una no conformidad, y<br>IV. Asegurar que aquéllos que requieran conocer sobre las potenciales no conformidades y las acciones preventivas implementadas. | IV. El responsable y/o encargado deberá contar con un listado del personal al que será necesario informar sobre las no conformidades y acciones preventivas. Posteriormente, deberá establecer procedimientos y/o mecanismos para asegurarse de que aquellos que requieran conocer sobre una potencial no conformidad y de la implementación de acciones preventivas, tengan conocimiento. |
| 15.2. Para la Implementación de acciones correctivas cuanto tenga lugar una no conformidad, el responsable deberá:<br>I. Prever procedimientos para revisar dicha no conformidad.<br>II. Eliminar, reducir o documentar la situación a detalle cuando se determine que la reducción en el grado de la no conformidad no puede garantizarse.<br>III. Procedimientos para corregir las no conformidades identificadas y un plazo límite para realizarlas.<br>IV. El aseguramiento que cualquier nuevo riesgo identificado para los datos personales sea evaluado con procesos proactivos, tales como las | I. El responsable y/o encargado deberá establecer procedimientos debidamente documentados para la revisión de la o las no conformidades que se generen en las auditorías, con el fin de analizar si es<br>II. El responsable y/o encargado cuando se genere una “no conformidad” deberá realizar y documentar las siguientes opciones, eliminar la causa de esta no conformidad, reducir el grado de la no conformidad, o bien, si no es posible reducir el grado de la no conformidad, documentar la situación a detalle cuando la reducción no pueda garantizarse.<br>III. Considerando lo anterior, el responsable y/o encargado deberá documentar los procedimientos y formatos que utilizará la organización para corregir las no conformidades identificadas, asimismo se deberán considerar criterios para los plazos límites que se deberán considerar para corregirlas.<br>IV. El responsable y/o encargado deberá documentar los procedimientos que le permita identificar aquellos nuevos riesgos que deban ser evaluados con procesos proactivos como pueden ser las evaluaciones de impacto a la privacidad, o aquellas buenas prácticas nacionales o internacionales. |

| | |
|---|---|
| evaluaciones de impacto a la privacidad. | |
| 15.3. Evaluar por el personal previamente asignado para tal caso, los cambios propuestos al SGDP o la Política, previo su implementación. | El responsable y/o encargado deberá evaluar previamente todos los cambios propuestos al SGDP y/o la Política, el personal que se ha designado para operar el SGDP es quien será el encargado de realizarlos.<br><br>Asimismo, se deberá establecer el procedimiento, mecanismo o metodología de evaluación que será utilizado, que puede incluir criterios previamente establecidos. |
| 15.4. Documentar y conservar conforme a los periodos establecidos para ello, los cambios derivados de las acciones preventivas y correctivas. | El responsable y/o encargado debe de establecer procedimientos para mantener documentado y conservar la información, conforme a los periodos establecidos para ello, referidos en el segundo punto del 14.1 (Conservar los resultados y las revisiones de las acciones implementadas). |
| **16. Sanciones** | |
| 16.1. Previstas cuando una no conformidad no haya sido corregida en los plazos establecidos para ello; aplicables a los causantes de dicha no conformidad; | El responsable y/o encargado deberá de establecer y documentar las sanciones que serán aplicadas cuando una no conformidad no haya sido corregida en los plazos establecidos para ello, determinados en el punto 14 (Requisitos relativos a las acciones preventivas y correctivas), además de que deberán ser aplicables a quienes se haya determinado como causante de la no conformidad. |
| 16.2 Consistentes en amonestaciones, sanciones económicas o suspensiones temporales o definitivas de la adhesión, entre otras. | El responsable y/o encargado deberá de establecer el tipo de sanciones que aplicará la organización, las cuales pueden ser amonestaciones, sanciones económicas o suspensiones temporales o definitivas de la adhesión, entre otras.<br><br>Asimismo, es relevante que se establezcan criterios para aplicar cada tipo de sanción. |
| 16.3. Pueden hacerse públicas. | El responsable y/o encargado podrá determinar si las sanciones serán públicas y por qué medios en su caso serán publicadas, en caso contrario, deberán establecer que no serán públicas, o bien, establecer un criterio para determinar cuáles serán públicas y cuáles no. |
| 16.4. Prever su notificación al adherido, cuando se trate de un esquema que aplique a un grupo de responsables o encargados | Cuando se trate de un grupo de responsables o encargados que formen parte del esquema, se deberá establecer un procedimiento y formato para notificar al adherido todas las sanciones correspondientes, establecidas previamente, asi como su fundamento. |
| **17. Mejora continua** | |

| | |
|---|---|
| 17.1. Mejora continua de la efectividad del SGDP considerando los resultados de las auditorías, las acciones preventivas y correctivas, y los resultados de las revisiones administrativas. | La organización debe mejorar de manera continua la idoneidad, adecuación y sobre todo la eficacia del SGDP, para ello deberá incluir y documentar las decisiones y acciones relacionadas con las oportunidades de mejora continua y cualquier cambio en el SGDP.<br><br>El responsable y/o encargado deberá realizar una mejora continua al SGDP considerando los resultados de las auditorías, las acciones preventivas y correctivas, así como los resultados en las revisiones administrativas.<br><br>En este sentido el responsable y/o encargado deberá documentar la implementación de acciones llevadas a cabo considerando los resultados de las auditorias, las acciones preventivas y correctivas, así como los resultados en las revisiones administrativas con el fin de dar seguimiento y atención a la mejora continua en todas las fases del SGDP. |
| 17.2 Además, se podrá considerar las quejas, vulneraciones de seguridad y solicitudes de acceso, entre otros. | El responsable y/o encargado podrá utilizar las quejas, vulneraciones de seguridad y solicitudes de acceso que se hayan presentado durante un periodo determinado, para la toma de decisiones de aquellas acciones necesarias para realizar una mejora continua en el SGDP. |