Protección de Datos Personales

Sistema de Gestión de Seguridad

Marco Normativo

APLICA

Sector Público Federal	Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
Ámbito Privado (a nivel nacional)	Ley Federal de Protección de Datos Personales en Posesión de los Particulares
Entidades Federativas	Leyes de protección de datos estatales

Objeto de la Ley

… establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados …

Artículo 1

Son sujetos obligados por esta Ley, en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.

Artículo 1

A Quienes no aplica la Ley

Los sindicatos y cualquier otra persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal serán responsables de los datos personales, de conformidad con la normatividad aplicable para la protección de datos personales en posesión de los particulares.

En todos los demás supuestos diferentes a los mencionados en el párrafo anterior, las personas físicas y morales se sujetarán a lo previsto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Artículo 1

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

Artículo 4

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;

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 presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;

Artículo 3 Fracc. IX, X

Titular: La persona física a quien corresponden los datos personales;

Responsable: Los sujetos obligados a que se refiere el artículo 1 de la presente Ley que deciden sobre el tratamiento de datos personales;

Encargado: La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable;

Artículo 4 Fracc. XXXI, XXVIII, XV

Conceptos

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 personale,

Bloqueo: La identificación y conservación de 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 de éstas. 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;

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;

Artículo 4 Fracc. IV, XXX, XXXIII

Deber de Seguridad

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.

Artículo 31

Deber de Seguridad

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.

Artículo 32

Deber de Seguridad

Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades 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 del responsable, entre otros;

Artículo 33

Deber de Seguridad

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.

Artículo 33

Deber de Seguridad

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.

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, de conformidad con lo previsto en la presente Ley y las demás disposiciones que le resulten aplicables en la materia.

Artículo 34

De manera particular, el responsable deberá elaborar un ***documento de seguridad*** que contenga, al menos, lo siguiente:

I. El inventario de datos personales y de los sistemas de tratamiento;
II. Las funciones y obligaciones de las personas que traten datos personales;
III. El análisis de riesgos;
IV. El análisis de brecha;
V. El plan de trabajo;
VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y
VII. El programa general de capacitación.

Artículo 35

Deber de Seguridad

El responsable deberá actualizar el documento de seguridad 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. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

Artículo 36

En caso de que ocurra una vulneración a la seguridad, 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.

Artículo 37

Deber de Seguridad

Además de las que señalen las leyes respectivas y la normatividad aplicable, se considerarán como vulneraciones de seguridad, en cualquier fase del tratamiento de datos, 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.

Artículo 38

Deber de Seguridad

El responsable deberá llevar una bitácora de las vulneraciones a la seguridad en la que se describa ésta, la fecha en la que ocurrió, el motivo de ésta y las acciones correctivas implementadas de forma inmediata y definitiva.

El responsable deberá informar sin dilación alguna al titular, y según corresponda, al Instituto y a los Organismos garantes de las Entidades Federativas, las vulneraciones que afecten de forma significativa los derechos patrimoniales o morales, en cuanto se confirme que ocurrió la vulneración y que el responsable 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.

Artículos 39 y 40

Deber de Seguridad

El responsable deberá informar al titular al menos lo siguiente:

I. La naturaleza del incidente;
II. Los datos personales comprometidos;
III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses;
IV. Las acciones correctivas realizadas de forma inmediata, y
V. Los medios donde puede obtener más información al respecto.

Artículo 41

Deber de Seguridad

El responsable deberá informar al titular al menos lo siguiente:

I. La naturaleza del incidente;
II. Los datos personales comprometidos;
III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses;
IV. Las acciones correctivas realizadas de forma inmediata, y
V. Los medios donde puede obtener más información al respecto.

Artículo 41

Deber de Seguridad

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.

Artículo 42

Inventario de Datos Personales

Dentro del deber de seguridad en el artículo 33 de la Ley, se establece la actividad de *“elaborar un inventario de datos personales y de los sistemas de tratamiento”*.

El cual se debe establecer y mantener actualizado. Este inventario debe identificar o estar vinculado con la información básica que permita conocer el tipo de tratamiento al que son sometidos los datos personales, la cual se relaciona de manera directa con su flujo o ciclo de vida, considerando:

- Obtención
- Almacenamiento
- Uso: Acceso, Manejo, Aprovechamiento, Monitoreo, Procesamiento
- Divulgación: Remisiones, Transferencias
- Bloqueo
- Cancelación, supresión o destrucción.

Inventario de Datos Personales

Por lo que dentro la elaboración del Inventario de Datos Personales se recomienda tratar de contestar los siguientes cuestionamientos:

- Si es sensible
- De dónde se obtienen los datos
- Qué personas de la organización están autorizados a tratar los datos personales
- Las finalidades del tratamiento de los datos personales
- Con quién se comparten los datos personales (encargados o transferencias) y para qué se comparten
- En dónde y cómo se almacenan los datos personales
- Los procedimientos, mecanismos y tecnología utilizada para su tratamiento
- Cuanto tiempo se conservan
- Procedimientos para su destrucción

Análisis de Riesgo

La seguridad se basa en el entendimiento de la naturaleza del riesgo al que están expuestos los datos personales, el riesgo no se puede erradicar completamente, pero sí se puede minimizar a través de la mejora continua.

Para poder definir un plan del riesgo a tratar y posteriormente implementar controles de seguridad, se deben tener diferentes criterios de evaluación dentro de la organización, que permitan delimitar el nivel de riesgo aceptable para los datos personales. Estos criterios de evaluación del riesgo de la seguridad de los datos personales deben considerar los factores establecidos en el artículo 31.

De manera adicional, entre otros factores que pueden incidir en el nivel de riesgo se encuentran los siguientes:

- Los requerimientos regulatorios y obligaciones contractuales que se usaron para definir los objetivos y alcances.
- El valor de los datos personales, de acuerdo a su clasificación por tipo definida previamente y su flujo.
- El valor y exposición de los activos involucrados con los datos personales.
- Expectativas de las partes interesadas, así como las consecuencias negativas a la reputación de la organización, que pudieran derivar de una vulneración.

Las organizaciones pueden establecer dos tipos de criterios de evaluación del riesgo, los de impacto y los de aceptación. Los primeros corresponden a todo el posible daño a los titulares, mientras que los de aceptación se alinean de manera general a los niveles de riesgo que una organización se fije como meta respecto a sus alcances y objetivos.

Estos criterios deberían estar formalmente documentados y ser utilizados como directriz para valorar el riesgo.

Análisis de Riesgo

La valoración del riesgo identifica los activos existentes, las amenazas aplicables, y los escenarios de vulneración. Asimismo, determina las consecuencias potenciales y prioriza los riesgos derivados respecto al contexto de la organización y los criterios de evaluación del riesgo.

Esta valoración del riesgo debe considerar:

- El establecimiento y mantenimiento de criterios de aceptación de riesgos.
- La determinación de los criterios para evaluar los riesgos.
- Asegurar que las diferentes evaluaciones del riesgo generen resultados consistentes validos y comparables.

Para la realización de esta valoración de Riesgo es necesario:

- Identificar Activos
- Identificar Amenazas
- Identificar Vulnerabilidades
- Identificar Escenarios de vulneración y consecuencias

Con base en el análisis de riesgos se deberán seleccionar e implementar las medidas de seguridad administrativas, técnicas o físicas que permitan disminuir los riesgos.

Análisis de Brecha

Una vez identificados los activos y procesos relacionados a los datos personales, así como las amenazas, vulnerabilidades y escenarios de incidentes relacionados, se puede proceder al análisis de brecha de las medidas de seguridad.

El análisis de brecha consiste en identificar:

- Las medidas de seguridad existentes
- Las medidas de seguridad existentes que operan correctamente
- Las medidas de seguridad faltantes
- Si existen nuevas medidas de seguridad que puedan remplazar a uno o más controles implementados actualmente.

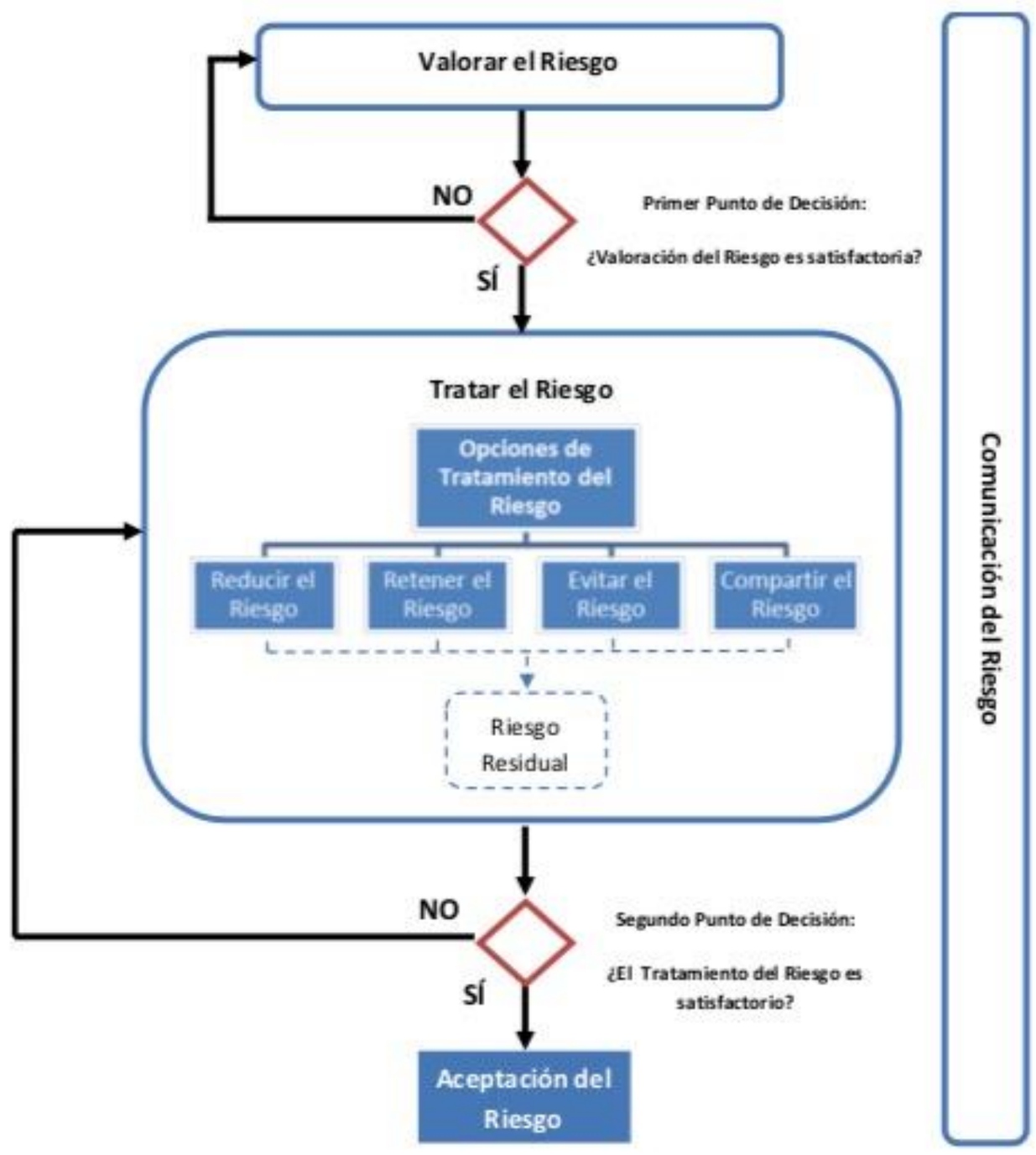
Análisis de Brecha

Es importante tener claro cuáles son los controles que ya están funcionando en una organización de manera efectiva, con su respectivo nivel de madurez, así como las medidas identificadas como faltantes, para constituir un programa de trabajo que refleje los recursos designados, los responsables, y las fechas compromiso para su implementación. De manera que se pueda medir la eficacia del SGSDP con respecto de los riesgos tratados.

Se deben seleccionar los controles de seguridad faltantes identificados en el análisis de brecha y en el plan de tratamiento del riesgo, tomando en cuenta la ponderación hecha en la valoración. Existen cuatro posibilidades comunes para tratar el riesgo: mitigar o reducir el riesgo, retener el riesgo, evitar el riesgo y compartir el riesgo.

Las opciones de tratamiento del riesgo deben ser seleccionadas con base en el resultado de la valoración del riesgo, los costos estimados, y los beneficios esperados de implementar estas opciones.

Plan de Trabajo para la Implementación de las Medidas Faltantes



Existen factores que pueden afectar la selección de controles. Limites técnicos, como requerimientos de rendimiento, capacidad de gestión y los asuntos de compatibilidad, pueden obstaculizar el uso de ciertos controles o pueden inducir a errores humanos nulificando el control, dando un falso sentido de seguridad o incrementando el riesgo más allá del control.

En el artículo 34 de la ley se establece que todas las acciones relacionadas con las medidas de seguridad para le tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión, definiendo el sistemas de gestión como:

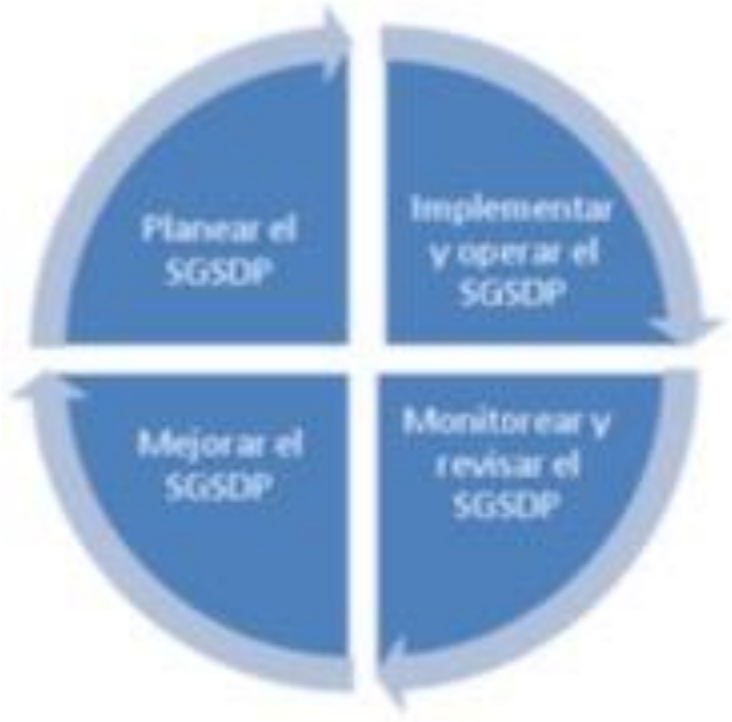
"… conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar mantener y mejorar el tratamiento y seguridad de los datos personales …"

La gestión es un conjunto de actividades coordinadas para dirigir y controlar un proceso o tarea.

Un sistema es un conjunto de elementos mutuamente relacionados o que interactúan por un fin u objetivo.

Por lo tanto, un Sistema de Gestión (SG) se define como un conjunto de elementos y actividades interrelacionadas para establecer metas y los medios de acción para alcanzarlas.

El sistema de gestion que establece la Ley a partir las acciones contenidas en el Capitulo II “De los Deberes”, se encuentra basado en el modelo denominado “Planificar – Hacer – Verificar – Actuar” (Plan – Do – Check - Act), basado en el Ciclo de Deming, el cual es una espiral de mejora continua.



	Elemento del SG	Fase del PHVA	Actividades
PROCESO	Metas	Planificar	Se identifican políticas, objetivos, riesgos, planes, procesos y procedimientos **necesarios para obtener el resultado esperado por la organización (meta).**
	Medios de acción	Hacer	Se implementan y operan las políticas, objetivos, planes, procesos y procedimientos **establecidos en la fase anterior.**
		Verificar	Se evalúan y miden **los resultados de las políticas, objetivos, planes, procesos y procedimientos implementados, a fin de verificar que se haya logrado la mejora esperada.**
		Actuar	Se adoptan medidas correctivas y preventivas, en función de los resultados y de la revisión, o de otras informaciones relevantes, para lograr la mejora continua.

Gracias

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Secretaría de Protección de Datos Personales

Dirección General de Investigación y Verificación del Sector Privado