GOBIERNO DE MÉXICO | FUNCIÓN PÚBLICA
SECRETARÍA DE LA FUNCIÓN PÚBLICA

Documento de Seguridad

EN MATERIA DE TRATAMIENTO DE DATOS PERSONALES EN POSESIÓN DE LA SECRETARÍA DE LA FUNCIÓN PÚBLICA

CONTENIDO

1. Introducción

A partir de la reforma constitucional de 2009, la protección de datos personales quedó establecida como un derecho fundamental en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, que reconoce que toda persona tiene derecho a la protección y al ejercicio de los derechos de acceso, rectificación, cancelación y oposición al tratamiento de sus datos personales.

Posteriormente, la reforma constitucional de 2014, en materia de transparencia, fortaleció los mecanismos de resguardo y estableció una directriz clara en el sentido de que todos los sujetos obligados deben garantizar medidas de seguridad adecuadas para la protección de los datos personales que poseen. En ese sentido, se otorgaron facultades al Congreso de la Unión para materializar el contenido de la reforma a través de leyes y así otorgarle "forma, alcance y sentido."

El 26 de enero de 2017 se expidió la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (en adelante Ley General), la cual tiene como objetivo establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales que estén en posesión de sujetos obligados.

"... son sujetos obligados 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"

Asimismo, en la Ley General se señala que son sujetos obligados, 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, así como sindicatos y cualquier otra persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad.[1]

[1] Sujeto obligado en términos de lo que establecen los artículos 1 y 3 (fracción XXVIII) de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

La Secretaría de la Función Pública (en adelante Secretaría), como parte del Ejecutivo Federal[2], es un sujeto obligado, en términos de la Ley General, responsable de decidir el tratamiento de los datos personales que se encuentran en su posesión.

Bajo esta óptica, la Secretaría a través de sus unidades administrativas es responsable de proteger los datos personales que trate, observando los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, así como los deberes de seguridad y confidencialidad y las demás obligaciones derivadas de la Ley General.

Estos principios, deberes, obligaciones y derechos imponen una serie de obligaciones para los responsables, que tienen como finalidad que el tratamiento se realice de tal manera, que se garantice la protección de los datos personales de sus titulares.

"La Secretaría para el ejercicio de sus unidades administrativas es responsable de proteger los datos personales que trate, observando los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad"

En relación con el deber de seguridad, la Ley General señala que el responsable del tratamiento deberá establecer y mantener 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[3].

Así, entre las actividades para acreditar el deber de seguridad se encuentra la obligación de elaborar un Documento de Seguridad[4], que en el contexto de protección de datos personales, se define como el instrumento que describe y da cuenta sobre las medidas de seguridad técnicas, físicas y administrativas implementadas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que poseen las distintas unidades administrativas.

[2] De conformidad con los artículos 2, 26 y 37 de la Ley Orgánica de la Administración Pública Federal.
[3] Artículo 31 de la Ley General
[4] Artículo 35 de la Ley General

Además, el Documento de Seguridad deberá contener al menos: 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 riesgo; 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 Anual de Capacitación[5].

"...un Documento de Seguridad, ..., se define como el instrumento que describe y da cuenta sobre las medidas de seguridad técnicas, físicas y administrativas implementadas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales"

De acuerdo con el Reglamento Interior de la Secretaría de la Función Pública (en adelante Reglamento Interior), la Unidad de Políticas Anticorrupción es la encargada de fungir como Titular de la Unidad de Transparencia, así como de presidir el Comité de Transparencia de la Secretaría, tomando en consideración los Lineamientos de actuación del Comité de Transparencia[6]. Para el ejercicio de sus atribuciones se apoya en la Dirección General de Transparencia y Gobierno Abierto[7](en lo sucesivo Dirección General), que, entre otras funciones, realiza las gestiones necesarias para cumplir con los acuerdos del Comité de Transparencia de la Secretaría[8], a través de las unidades administrativas que le auxilian.

Conforme a sus atribuciones, la Dirección General coordinó la actualización[9] del presente Documento de Seguridad, que consistió en las siguientes actividades:

- El 17 de enero de 2024, el Comité de Transparencia tomó conocimiento del Plan de Trabajo para la actualización del Documento de Seguridad.
- El 19 de abril de 2024 se remitieron oficios a los titulares de las unidades administrativas de la Secretaría, para informarles que iniciarían los trabajos para realizar la actualización del Documento de Seguridad.

[5] Artículo 35 de la Ley General.
[6] Artículo 186, fracción III, inciso b) del Reglamento Interior.
[7] Artículo 188, fracción IV del Reglamento Interior.
[8] Con fundamento en el artículo 188, fracción IV y V del Reglamento Interior.
[9] Artículo 36 de la Ley General.

- El 24 de abril de 2024 se presentó ante el Comité de Transparencia el calendario de actividades, en materia de datos personales, para cumplir con las obligaciones de la Ley General, en donde se incluyó la actualización del Documento de Seguridad.
- Se diseñó la herramienta para la captura de información, denominada Matriz de información, para la elaboración del Documento de Seguridad, la cual incluye, a diferencia del formato proporcionado por el Instituto Nacional de Transparencia y Protección de Datos Personales (INAI), el inventario de datos y sistemas de tratamiento, el catálogo de activos, el análisis de riesgo y brecha, y el Plan de Trabajo.
- Se realizaron seis talleres prácticos, los días 7, 8, 9, 22, 23 y 24 de mayo de 2024, con los enlaces designados en las unidades administrativas para proporcionarles la información necesaria para la captura de datos en la Matriz de información para la elaboración del Documento de Seguridad.

"La Matriz de información para la elaboración del Documento de Seguridad contiene el inventario de datos y sistemas de tratamiento, el catálogo de activos, el análisis de riesgo y brecha y el Plan de Trabajo"

De esta forma, las distintas unidades administrativas que consideraron contar con tratamientos de datos personales, entregaron a la Dirección General la *Matriz de información para la elaboración del Documento de Seguridad*, con los elementos requeridos en la Ley General y los Lineamientos Generales de Protección de Datos Personales para el Sector Público (en lo sucesivo Lineamientos Generales).

2. Glosario

En adición a los términos establecidos en el artículo 3 de la Ley General, para efectos del presente documento, se entenderá por:

Anexo Técnico. - Análisis realizado por la Dirección de Seguridad de Tecnologías de Información adscrita a la Dirección General de Tecnologías de la Información (DGTI)

Anexo Análisis de Medidas de Seguridad. - Integración del análisis realizado a la información remitida por las unidades administrativas, en cuanto a las medidas de seguridad administrativas, físicas, técnicas y el plan de trabajo a realizar.

Anexo Plan de Capacitación. - Plan Anual de Capacitación, en materia de protección de datos personales, aprobado por el Comité de Transparencia el 22 de mayo del 2024.

Ciclo de vida.- Se refiere a las fases del tratamiento de los datos personales, consistentes en la obtención, almacenamiento, uso, divulgación, bloqueo y cancelación.[10]

Comité de Transparencia. - Autoridad máxima en materia de protección de datos personales.[11]

Deberes.- Confidencialidad y seguridad.[12]

Inventario de datos personales. - Identificación de las bases de datos de tratamiento de las unidades administrativas, por el cual se documenta la información básica de cada tratamiento realizado, con independencia de su forma de almacenamiento, entre lo que se incluye el ciclo de vida del dato personal.

Ley General. - Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Lineamientos Generales. - Lineamientos Generales de Protección de Datos Personales para el Sector Público.

[10] De conformidad con el artículo 59 de los Lineamientos Generales.
[11] De conformidad con el artículo 83 de la Ley General.
[12] Deber de seguridad de conformidad con los artículos 31, 32, 33, 34, 35 y 36 de la Ley General y 55 al 65 de los Lineamientos Generales; deber de confidencialidad bajo a lo dispuesto en el artículo 42 de la Ley General y 71 de los Lineamientos.

Principios. - Reglas que guían la protección de datos personales y definen las obligaciones que tienen los responsables del tratamiento con relación al uso y cuidado de los datos personales, que, al mismo tiempo, se traducen en los derechos de aquellos titulares que les han entregado sus datos.

El derecho a la protección de los datos personales se regula a través de ocho principios, los cuales se traducen en obligaciones, estos son: licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales.

Reglamento Interior. - Reglamento Interior de la Secretaría de la Función Pública.

Sistemas. - Conjunto de elementos mutuamente relacionados o que interactúan por un fin u objetivo.

Titular de la Unidad Administrativa.- Persona responsable del tratamiento de los datos personales en la unidad administrativa a su cargo de conformidad al artículo 6 del Reglamento Interior de la Secretaría de la Función Pública.[13]

Unidad Administrativa. - Las previstas en el artículo 7 del Reglamento Interior de la Secretaría de la Función Pública.

[13] Artículo 6del Reglamento Interior de la Secretaría de la Función Pública. Las personas titulares de las unidades administrativas de la Secretaría ejercen el mando directo sobre aquellas cuyas unidades administrativas les sean adscritas de conformidad con este reglamento o el acuerdo de adscripción que se emita en términos del artículo 16 de la Ley Orgánica de la Administración Pública Federal.

3. Marco normativo

- Constitución Política de los Estados Unidos Mexicanos, artículos 6°, Base A y 16, segundo párrafo.
- Ley General de Transparencia y Acceso a la Información Pública.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Ley Orgánica de la Administración Pública Federal.
- Reglamento Interior de la Secretaría de la Función Pública.
- Lineamientos Generales de Protección de Datos Personales para el Sector Público.
- Lineamientos que establecen los parámetros, modalidades y procesamiento para la portabilidad de datos personales.
- Guía para cumplir con los principios y deberes de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Lineamientos de actuación del Comité de Transparencia.
- Política Interna de Protección de Datos Personales de la Secretaría de la Función Pública.
- Guía de apoyo para la elaboración del documento de seguridad.
- Metodología de Análisis de Riesgo BAA.

4. Ámbito de aplicación y observaciones generales

En atención a los deberes que establece la Ley General, el presente documento es aplicable para todas las unidades administrativas de la Secretaría que, en el ejercicio de sus atribuciones y funciones, administren sistemas físicos y/o electrónicos de tratamientos de datos personales, ya sea que operen sistemas completos o el tramo de información que le corresponda.

Asimismo, serán aplicables al tratamiento de datos personales que obren en soportes físicos y/o electrónicos, con independencia de la forma o modalidad de su creación, procesamiento, almacenamiento y organización.

"... las personas titulares de las direcciones generales tienen la facultad de establecer las medidas necesarias que garanticen la seguridad de los datos personales que en el ámbito de su competencia posean, recaben o transmitan, a fin de evitar su alteración, pérdida, transmisión y acceso no autorizado,"

Todas las personas servidoras públicas y encargadas que tengan acceso a los datos personales están obligadas a conocer y aplicar las medidas de seguridad propias de cada sistema en el que se concentren los datos y es aplicable en todas y cada una de las fases del tratamiento de los datos personales, iniciando desde la obtención de los mismos y finalizando con su supresión. Cabe mencionar que, la obligación de confidencialidad debe subsistir durante y después de que los involucrados hayan finalizado su participación en el tratamiento de los datos personales, porque hayan cambiado de funciones y también cuando la relación laboral con la Secretaría haya concluido.

5. Inventario, funciones y obligaciones de las personas que tratan datos personales

Los artículos 33, fracción III de la Ley General y; 58 de los Lineamientos Generales establecen que se elabore un inventario de datos personales, como una medida de seguridad para la protección de los mismos.

El inventario de datos personales es la identificación de las bases de datos de tratamiento de las unidades administrativas de la Secretaría, en donde se documenta la información básica de cada tratamiento realizado, con independencia de su forma de almacenamiento, entre lo cual, se incluye el ciclo de vida del dato personal.

De esta manera, como ya se mencionó, el inventario de datos personales, así como las funciones y obligaciones forman parte del documento de seguridad, señalado en el artículo 35, fracciones I y II de la Ley General. En este sentido, a continuación, se detalla el inventario, funciones y obligaciones de las bases de datos reportadas por las unidades administrativas de la Secretaría, que se encuentran tanto en soporte electrónico, como físico.

En correlación con el precepto legal antes citado, los artículos 58 y 59 de los Lineamientos Generales establecen lo siguiente:

Inventario de datos personales

Artículo 58. Con relación a lo previsto en el artículo 33, fracción III de la Ley General, el responsable deberá elaborar un inventario con la información básica de cada tratamiento de datos personales, considerando, al menos, los siguientes elementos:

I. El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales;
II. Las finalidades de cada tratamiento de datos personales;
III. El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no;
IV. El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales;
V. La lista de servidores públicos que tienen acceso a los sistemas de tratamiento;
VI. En su caso, el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable, y
VII. En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican éstas.

Ciclo de vida de los datos personales en el inventario de éstos

Artículo 59. Aunado a lo dispuesto en el artículo anterior de los presentes Lineamientos generales, en la elaboración del inventario de datos personales el responsable deberá considerar el ciclo de vida de los datos personales conforme lo siguiente:

I. La obtención de los datos personales;

II. El almacenamiento de los datos personales;

III. El uso de los datos personales conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin;

IV. La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen;

V. El bloqueo de los datos personales, en su caso, y

VI. La cancelación, supresión o destrucción de los datos personales.

El responsable deberá identificar el riesgo inherente de los datos personales, contemplando su ciclo de vida y los activos involucrados en su tratamiento, como podrían ser hardware, software, personal, o cualquier otro recurso humano o material que resulte pertinente considerar.

A partir de lo anterior, la Dirección General a través de la Dirección de Protección de Datos Personales trabajó junto con las unidades administrativas adscritas a la Secretaría para la construcción de inventarios de los distintos tratamientos de datos personales que realizan cada una de ellas, cuya premisa general fue la coordinación interna para localizar todos los procesos en los que exista tratamiento de datos personales en posesión de la Secretaría de la Función Pública. Este proceso se hizo identificando los elementos informativos que señala el artículo 58 de los Lineamientos Generales y con base en el ciclo de vida de los datos personales, como lo señala el artículo 59 de los Lineamientos Generales.

Finalmente, cabe señalar que los inventarios forman parte integral del presente documento de seguridad.

De conformidad con los artículos 33, fracción II y III, y 35, fracción II de la Ley General y; 57, 58 y 59 de los Lineamientos Generales, se desarrollan los inventarios, funciones y obligaciones de las personas que tratan datos personales en la Secretaría. Lo reportado por las unidades administrativas se podrá observarse en el ANEXO I del presente documento el cual será actualizado para dar cumplimiento con lo señalado en el artículo 36 de la Ley General, mismo que establece que:

> Artículo 36. 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.

De esta forma, el artículo 33, fracción II de la Ley General establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, la definición de las funciones y obligaciones del personal involucrado en el tratamiento de datos personales.

Como se señaló, de acuerdo con la fracción II del artículo 35 de la Ley General, este elemento informativo forma parte del documento de seguridad.

Sobre el particular, el artículo 57 de los Lineamientos Generales señala lo siguiente:

> ***Funciones y obligaciones***
> ***Artículo 57.*** *Con relación a lo dispuesto en el artículo 33, fracción II de la Ley General, el responsable deberá establecer y documentar los roles y responsabilidades, así como la cadena de rendición de cuentas de todas las personas que traten datos personales en su organización, conforme al sistema de gestión implementado.*
>
> *El responsable deberá establecer mecanismos para asegurar que todas las personas involucradas en el tratamiento de datos personales en su organización, conozcan sus funciones para el cumplimiento de los objetivos del sistema de gestión, así como las consecuencias de su incumplimiento.*

6. Medidas de Seguridad

Las medidas de seguridad son elementos de control que tienen el objetivo de garantizar la confidencialidad, integridad y disponibilidad de la información. En el caso de los datos personales, las medidas de seguridad se implementan a lo largo de su ciclo de vida para evitar que los datos sean expuestos, alterados o bloqueados por personas o entidades no autorizadas.[14]

Las medidas de seguridad se clasifican por su naturaleza en:

I. Administrativas

II. Físicas

III. Tecnológicas

Así, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, (artículos 31 y 33) y sus Lineamientos Generales (artículo 55), mandatan que los responsables de los datos personales deberán establecer y mantener medidas de seguridad de carácter administrativas, físicas y técnicas para su protección, que permitan resguardarlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

De la misma forma, para establecer y mantener las medidas de seguridad para la protección de datos personales, se deberá de realizar, al menos, las siguientes actividades relacionadas:

a) 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;
b) Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales;
c) Elaborar un inventario de datos personales y de los sistemas de tratamiento;
d) 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;

[14] Fragoso Rodríguez, Uciel, Diccionario de Datos Personales, Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), 2019, p.555.

e) Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;
f) 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;
g) 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
h) 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.

Bajo esta óptica, las medidas de seguridad se describen de la siguiente manera:

Las medidas de seguridad administrativas: Corresponden a todas las acciones encaminadas a la protección de la información y que están relacionadas con la gente y los procesos

La Ley General[15] establece que son las políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal en datos personales.

Las medidas de seguridad físicas: Refieren a todos los controles que tienen como objetivo asegurar el acceso físico a la información y a todo su entorno En la Ley General[16] se establece que son el conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento, en los que se pueden considerar las siguientes actividades:

a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y

[15] Artículo 3, fracción XXI, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados,
[16] Artículo 3, fracción XXII, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados,

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

Las medidas de seguridad tecnológicas: Refieren a todas las acciones apoyadas de infraestructura tecnológica (hardware y software) que intervienen en la creación, procesamiento, transmisión o almacenamiento de la información. La Ley General[17] las define como el conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento, se deben considerar las siguientes actividades:

a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;
b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y
d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Conforme a lo anterior, la Secretaría de la Función Pública, a través de sus unidades administrativas, es responsable de la protección y confidencialidad de los datos personales que recaba para realizar sus funciones, por lo tanto, tiene la obligación de establecer las medidas de seguridad antes enunciadas. Para lograrlo, se deben identificar las medidas de seguridad específicas que existen en cada una de las unidades administrativas en su entorno cotidiano y encausar la implementación de aquellas adicionales que se requieran para garantizar la efectiva protección de los datos personales.

[17] Artículo 3, fracción XXIII, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados,

7. Análisis de Riesgo y Brecha [18]

Para generar los mecanismos de seguridad se deben identificar peligros y estimar riesgos, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, a través de un análisis cualitativo sobre el impacto y la probabilidad de que una amenaza vulnere la seguridad de los datos personales, considerando lo siguiente:

a. Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico;
b. El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida;
c. El valor y exposición de los activos involucrados en el tratamiento de los datos personales;
d. Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida;
e. El riesgo inherente a los datos personales tratados;
f. La sensibilidad de los datos personales tratados;
g. El desarrollo tecnológico;
h. Las posibles consecuencias de una vulneración para los titulares;
i. Las transferencias de datos personales que se realicen;
j. El número de titulares;
k. Las vulneraciones previas ocurridas en los sistemas de tratamiento, y
l. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener datos personales tratados para una tercera persona no autorizada para su posesión.

De esta forma, el artículo 33, fracciones IV, V y VI de la Ley General establecen como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, la realización del análisis de riesgo, análisis de brecha y plan de trabajo, en los siguientes términos:

[18] Artículos 60 y 61 de los Lineamientos Generales

Artículo 33. 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. [...]

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;

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;

Por su parte, los artículos 60, 61 y 62 de los Lineamientos Generales establecen lo siguiente:

Análisis de riesgos

Artículo 60. Para dar cumplimiento al artículo 33, fracción IV de la Ley General, el responsable deberá realizar un análisis de riesgos de los datos personales tratados considerando lo siguiente:

I. Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico;
II. El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida;
III. El valor y exposición de los activos involucrados en el tratamiento de los datos personales;
IV. Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida, y
V. Los factores previstos en el artículo 32 de la Ley General.

Análisis de brecha

Artículo 61. Con relación al artículo 33, fracción V de la Ley General, para la realización del análisis de brecha el responsable deberá considerar lo siguiente:

I. Las medidas de seguridad existentes y efectivas;
II. Las medidas de seguridad faltantes, y
III. La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.

Como se señaló anteriormente, de acuerdo con las fracciones III, IV y V del artículo 35 de la Ley General, los análisis de riesgo y brecha y el plan de trabajo forman parte del documento de seguridad, cuya metodología para el análisis de riesgo toma como referencia la "Metodología de Análisis de Riesgo BAA"[19], que sustenta el ejercicio de análisis de riesgo realizado por las unidades administrativas de la Secretaría.

Para el análisis de brecha se contemplaron las siguientes medidas: I) de seguridad existentes y efectivas, II) de seguridad faltantes y III) la existencia de nuevas medidas de seguridad que pudieran remplazar a las actuales.

De lo anterior, cabe destacar que el análisis de brecha se refiere al proceso de evaluación de las medidas de seguridad administrativas, físicas y técnicas y las que operan correctamente en la Secretaría, contra las que serían necesarias tener para mitigar los riesgos de seguridad identificados en el análisis previo, así como las nuevas medidas de seguridad que podrían reemplazar a uno o más controles implementados actualmente.

[19] INAI, Metodología de Análisis de Riesgo BAA, 2015.

8. Plan de trabajo[20]

Una vez realizados los análisis de riesgo y el análisis de brecha, se elaboró un plan de trabajo por cada base de datos, con la finalidad de implementar las medidas de seguridad más relevantes e inmediatas a establecer, así como para el cumplimiento cotidiano de las políticas de tratamiento de los datos personales; priorizando las medidas de seguridad más relevantes e inmediatas a establecer, así como el tiempo, el entregable y el área a cargo de su cumplimiento y para su implementación.

Cabe señalar que de conformidad con el Anexo 8 de la Metodología, criterios, formatos e indicadores en materia de evaluación del desempeño de los responsables respecto al cumplimiento de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás disposiciones que resulten aplicables en observancia del artículo 250 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, el Documento de Seguridad se deberá publicar en versión pública, **en el que se deberá testar el plan de trabajo, así como el análisis de riesgo y brecha,** lo que implica que en caso de que se dejen visibles, sin excepción, será considerado como incumplimiento al criterio de evaluación correspondiente que para tal efecto realice el INAI.

[20] Artículo 62 de los Lineamientos Generales

9. Mecanismos de monitoreo y revisión de las medidas de seguridad

El artículo 33, fracción VII, de la Ley General establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, el monitoreo y revisión de manera periódica de las medidas de seguridad implementadas, al igual que las amenazas y vulneraciones a las que están sujetos los datos personales.

Como se señaló anteriormente, de acuerdo con la fracción VI del artículo 35 de la Ley General, los mecanismos de monitoreo y revisión forman parte del documento de seguridad.

Así, respecto a los mecanismos de monitoreo y revisión de las medidas de seguridad, el artículo 63 de los Lineamientos Generales señala lo siguiente:

> **Monitoreo y supervisión periódica de las medidas de seguridad implementadas**
>
> **Artículo 63.** Con relación al artículo 33, fracción VII de la Ley General, el responsable deberá evaluar y medir los 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 propuestos y, en su caso, implementar mejoras de manera continua.
>
> Para cumplir con lo dispuesto en el párrafo anterior del presente artículo, el responsable deberá monitorear continuamente lo siguiente:
>
> **I.** Los nuevos activos que se incluyan en la gestión de riesgos;
> **II.** Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras;
> **III.** Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;
> **IV.** La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;
> **V.** Las vulnerabilidades identificadas para determinar aquéllas 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 ocurridas.
>
> Aunado a lo previsto en las fracciones anteriores del presente artículo, el responsable deberá contar con un programa de auditoría, interno y/o externo, para monitorear y revisar la eficacia y eficiencia del sistema de gestión.

Derivado de lo anterior, es posible identificar que el monitoreo y revisión de las medidas de seguridad tienen el objetivo de fortalecer, a través de un ciclo de mejora continua, la protección de los datos personales que resguarda esta Secretaría.

Para la protección de datos personales de los sistemas relacionados en el inventario de datos personales, se realizará un monitoreo y se revisarán de manera periódica las medidas de seguridad actuales y las implementadas, así como las amenazas y vulneraciones a las que puedan estar sujetos los datos personales, de conformidad con el plan a cargo de la Dirección General de Tecnologías de la Información.

Para cumplir con lo anterior, el responsable deberá monitorear continuamente lo siguiente:

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

2. Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras.

3. Las nuevas amenazas que podrían estar activas dentro y fuera del sujeto obligado y que no han sido valoradas.

4. La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes.

5. Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir.

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

7. Los incidentes y vulneraciones de seguridad ocurridos.

Asimismo, el responsable deberá contar con un programa de supervisión y vigilancia interna para comprobar el cumplimiento de las políticas de protección de datos personales. Es por ello que la Secretaría elaboró el siguiente mecanismo para dar cumplimiento con dichas obligaciones.

A. MONITOREO

La Dirección General a través de la Dirección de Protección de Datos Personales será la encargada de ejecutar el mecanismo de monitoreo y supervisión autorizado por el Comité de Transparencia de conformidad con el artículo 122, fracciones II y III de los Lineamientos Generales. Las medidas de seguridad implementadas en la protección de datos personales serán monitoreadas a través del siguiente formato, el cual será enviado a las áreas de forma trimestral para conocer el estado en el que se encuentran sus sistemas de tratamiento.

Formato de monitoreo

Reactivos	Sí	No
1. Se han definido y se establecen y mantienen las medidas de seguridad administrativas, técnicas y físicas necesarias para la protección de los datos personales.	☐	☐
2. Se ha revisado el marco normativo que regula en lo particular el tratamiento de datos personales en cuestión, a fin de identificar si éste contempla medidas de seguridad específicas o adicionales a las previstas en la LGPDPPSO y los Lineamientos Generales, y se ha definido la procedencia de su implementación.	☐	☐
3. Se han definido las funciones, obligaciones y cadena de mando de cada servidor público que trata datos personales, por unidad administrativa.	☐	☐
4. Se ha comunicado a cada servidor público sus funciones, obligaciones y cadena de mando con relación al tratamiento de datos personales que efectúa.	☐	☐
5. Se ha elaborado el inventario de datos personales con los siguientes elementos: • **El catálogo de medios físicos y electrónicos, a través de los cuales se obtienen los datos personales;** • **Las finalidades de cada tratamiento de datos personales;** • **El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no;** • **El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales;** • **La lista de servidores públicos que tienen acceso a los sistemas de tratamiento;** • **En su caso, el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable, y** • **En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que las justifican.**	☐	☐

6. En el inventario de datos personales se tomó en cuenta el ciclo de vida de los datos personales, conforme a lo siguiente: • **La obtención de los datos personales;** • **El almacenamiento de los datos personales;** • **El uso de los datos personales conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin;** • **La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen;** • **El bloqueo de los datos personales, en su caso, y** • **La cancelación, supresión o destrucción de los datos personales.**	☐	☐
7. Se ha realizado el análisis de riesgo, considerando lo siguiente: • **Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico;** • **El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida;** • **El valor y exposición de los activos involucrados en el tratamiento de los datos personales;** • **Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida;** • **El riesgo inherente a los datos personales tratados, contemplando el ciclo de vida de los datos personales, las amenazas y vulnerabilidades existentes para los datos personales y los recursos o activos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal o cualquier otro recurso humano o material, entre otros;** • **La sensibilidad de los datos personales tratados;** • **El desarrollo tecnológico;** • **Las transferencias de datos personales que se realicen;** • **El número de titulares;** • **Las vulneraciones previas ocurridas en los sistemas de tratamiento, y** • **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.**	☐	☐
8. Se ha realizado el análisis de brecha, tomando en cuenta lo siguiente: • **Las medidas de seguridad existentes y efectivas;** • **Las medidas de seguridad faltantes, y** • **La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.**	☐	☐
10. Se monitorean y revisan, de manera periódica, las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, tomando en cuenta lo siguiente: • **Los nuevos activos que se incluyan en la gestión de riesgos;** • **Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras;**	☐	☐

- **Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;**
- **La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;**
- **Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;**
- **El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y**
- **Los incidentes y vulneraciones de seguridad ocurridas.**

La Dirección General a través de la Dirección de Protección de Datos Personales analizará los reportes de las áreas, verificando aquellos puntos en los que se hubiera reportado "No" como respuesta y se emitirá un dictamen en el que se plasmarán las recomendaciones o requerimientos que se consideren pertinentes en materia de seguridad, con la finalidad de que las áreas las atiendan y remitan las evidencias de su cumplimiento.

B. ACTUACIÓN ANTE VULNERACIONES

El artículo 33, fracción VII, de la Ley General, dispone que, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá 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.**

En ese sentido, el artículo 63, fracción VII, de los Lineamientos Generales, entre otras disposiciones estipula que, para evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, **se deberán monitorear las vulneraciones de seguridad ocurridas.**

Por ello, es necesario contar con un mecanismo que permita monitorear las alertas de seguridad de los datos personales, como posibles incidentes de seguridad, mismo que se desarrollará a través de las siguientes actividades:

1. Verificar si el hecho o evento podía dar como consecuencia una vulneración a la seguridad (posible incidente de seguridad), esto es:

   - Que exista una amenaza que, **de haberse concretado**, hubiera producido sus efectos en el tratamiento de los datos personales.
   - Que dichos efectos, **de haberse materializado**, hubieran representado un daño en los activos.

2. El área que advirtió de la alerta de seguridad deberá enviar un reporte a la Unidad de Transparencia, en un plazo no mayor a 72 horas, de conformidad con el artículo 66 de los Lineamientos Generales en el que deberá informar:

   - Circunstancias de modo, tiempo y lugar en que se detectó la amenaza.
   - Sistema de Tratamiento de Datos Personales, conforme al inventario, en el que se detectó la amenaza.
   - Datos personales involucrados.
   - Datos de identificación y de contacto de la persona servidora pública responsable del tratamiento de los datos personales.
   - Actuaciones que pueden evitar la explotación de la amenaza.
   - Descripción de los controles físicos o electrónicos involucrados en la amenaza.

3. El Oficial de Protección de Datos Personales registrará la alerta de seguridad e informará a la unidad responsable del tratamiento y al Comité de Transparencia para que en su caso se analice el impacto de la amenaza y, de ser posible, determinar una estrategia de prevención, en la que participen las áreas técnicas y normativas de la Secretaría, con la finalidad de evitar que la alerta de seguridad pueda desencadenarse.

C. SUPERVISIÓN Y VIGILANCIA INTERNA

Entre los mecanismos que se deben adoptar para cumplir con el principio de responsabilidad, el artículo 30, fracción V, de la Ley General de Datos Personales en Posesión de Sujetos Obligados establece que se deberá mantener un sistema de supervisión y vigilancia, que permita comprobar el cumplimiento de las políticas de datos personales.

10. Programa de capacitación

La Secretaría de la Función Pública, a través de la Dirección, promueve, coordina y opera la capacitación de las personas servidoras públicas en materia de protección de datos personales.

Así, en el artículo 188, fracción VI, del Reglamento Interior de la Secretaría de la Función Pública faculta a la Dirección General a coordinar y establecer los programas de capacitación continua y especializada en materia de transparencia, acceso a la información pública, gobierno abierto, rendición de cuentas, datos abiertos y protección de datos personales.

Asimismo, de conformidad con el artículo 30, fracción III, el artículo 33, fracción VIII, y los artículos 83 y 84, fracción VII, de la Ley General, así como los artículos 48 y 64 de los Lineamientos Generales, se dispone que el responsable deberá poner en práctica un programa de capacitación y actualización del personal sobre obligaciones y demás deberes en materia de protección de datos personales, aunado a esto, **el Comité de Transparencia es la autoridad máxima en materia de protección datos personales** y entre sus atribuciones se encuentra establecer programas de capacitación y actualización para las y los servidores públicos en materia de protección de datos personales.

Además, el artículo 10, fracción IX, de los Lineamientos de Actuación del Comité de Transparencia de la Secretaría de la Función Pública también establece que le corresponde al Comité de Transparencia vigilar la implementación de programas de capacitación en materia de protección de datos personales.

Por lo anterior, el 22 de mayo de 2024 se aprobó por el Comité de Transparencia el *Programa de Capacitación en Transparencia, Acceso a la Información, Protección de Datos Personales y Temas Relacionados* por el Comité de Transparencia, el cual fue presentado ante el INAI el 27 de mayo del mismo año.

Las acciones incluidas en el programa, citado en el párrafo anterior, tienen el objetivo de capacitar y concientizar a las y los servidores públicos de la Secretaría de la Función Pública para el mejor desempeño de sus atribuciones, la especialización de sus funciones, el óptimo cumplimiento de los objetivos institucionales y promoción de la profesionalización en el servicio público.

Las acciones específicas se muestran en el Anexo II del presente Documento de Seguridad.

11. Actualizaciones y aprobación

El artículo 36 de la Ley General establece la obligación de la actualización del 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. Se lleven a cabo acciones correctivas y preventivas ante una vulneración de seguridad.

Es por ello que el Comité de Transparencia deberá estar atento a la actualización de alguno de los supuestos antes señalados, para, en su caso, actualizar el presente documento de seguridad.

"... el pasado cuatro de septiembre de dos mil veintitrés se publicó en el Diario Oficial de la Federación la Reforma al Reglamento Interior de la Secretaría de la Función Pública en el que se realizaron cambios significativos en la organización"

Derivado de lo anterior, el 4 de septiembre de 2023 se publicó en el Diario Oficial de la Federación la Reforma al Reglamento Interior, en el que se realizaron cambios significativos en la estructura lo que implicó la necesidad de implementar acciones de mejora y actualización en el tratamiento de datos personales.

Al respecto, se realizaron las actividades necesarias para integrar la presente actualización del Documento de Seguridad, mismo que el Comité de Transparencia de la Secretaría de la Función Pública aprobó por unanimidad de sus integrantes en la Vigésima Séptima Sesión Ordinaria de 2024, celebrada el 17 de julio de 2024.

Fecha de actualización	Motivo de la actualización
12/06/2018	Aprobación del Documento de Seguridad de la Secretaría de la Función Pública.
10/11/2021	Dar cumplimiento a lo ordenado por el INAI en los procesos de verificación INAI.3S.07-01-004/2020 e INAI.3S.07-01-005/2020
17/07/2024	Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión.

Grethel Pilgram Santos

Suplente del Presidente del Comité de Transparencia

Mtra. María de la Luz Padilla Díaz

Titular del Área Coordinadora de Archivos

L.C. Carlos Carrera Guerrero

Suplente del Titular del Órgano Interno de Control

Elaboró e integró: Irving Manchinelly Mota, Director de Protección de Datos Personales, Oficial de Protección de Datos Personales de la Secretaría de la Función Pública

La presente foja forma parte integral del Documento de Seguridad aprobado por el Comité de Transparencia en la Vigésima Séptima Sesión Ordinaria del 2024, constante de veintiocho fojas útiles.