DOCUMENTO DE SEGURIDAD

Contenido

Introducción

El 26 de enero de 2017 se expidió la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (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 los sujetos obligados.

En su artículo primero, la Ley General 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.

La Ley General dispone que el tratamiento de datos personales que realicen los sujetos obligados esté regido por principios y deberes. Los principios son: licitud, lealtad, información, consentimiento, finalidad, proporcionalidad, calidad y responsabilidad; mientras que los deberes son el de confidencialidad y seguridad.

Asimismo, la Ley General detalla el alcance y los procedimientos para el ejercicio de los cuatro derechos que el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos reconoce a los titulares de los datos personales: acceso, rectificación, cancelación y oposición (derechos ARCO), y reconoce uno más, el de portabilidad.

Estos principios, deberes y derechos imponen una serie de obligaciones para los sujetos regulados por la Ley General, que tienen como finalidad que el tratamiento se realice de manera tal que se garantice la protección de los datos personales, con el objeto de respetar el derecho a la autodeterminación informativa de los titulares.

En específico, con relación al deber de seguridad, el artículo 31, de 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.

Al respecto, el artículo 33 de la Ley General señala lo siguiente:

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. *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;*
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.*

Por su parte, el artículo 35, de la Ley General establece como una obligación la elaboración de un **documento de seguridad**, que se define -según la fracción XIV, del artículo 3 de la Ley General- como *el "instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee".*

De conformidad con el artículo 35, de la Ley General, el documento deberá contener, al menos, la siguiente información:

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

En ese sentido, en cumplimiento de las obligaciones antes descritas, a continuación, se presenta el **Documento de Seguridad del Servicio de Protección Federal** (SPF) con los elementos informativos que establece el artículo 35, de la Ley General.

I. El inventario de datos personales y de los sistemas de tratamiento

El artículo 33, fracción I 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 elaboración de un inventario de datos personales y de los sistemas de tratamiento.

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

Sobre el particular, los artículos 58 y 59, de los Lineamientos Generales de Protección de Datos Personales para el Sector Público (en lo sucesivo, 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, el Servicio de Protección Federal elaboró los inventarios de los distintos tratamientos de datos personales que realiza, identificando los elementos informativos que señala el artículo 58, de los Lineamientos Generales y basados en el ciclo de vida de los datos personales, como lo requiere el artículo 59, de los Lineamientos Generales.

Los inventarios forman parte integral del presente documento de seguridad.

Con independencia de lo anterior, el siguiente cuadro muestra un resumen de los inventarios elaborados:

No.	Áreas	No. inventarios entregados	Nombre del tratamiento
1	Dirección General de Asuntos Jurídicos	13	1. Proceso de Trámite a solicitudes de Acceso a la información y Datos Personales.
			2. Proceso de Intervención en Recursos de Revisión
			3. Proceso de Juicios Amparo Administrativos
			4. Proceso de Juicios Amparo Penales
			5. Proceso de Juicios de Nulidad
			6. Proceso de Juicios Laborales
			7. Proceso de Juicios Civiles
			8. Proceso de Requerimientos Judiciales y Administrativos
			9. Proceso de Derechos de Petición

			10. Proceso de Atención a peticiones, sugerencias y quejas
			11. Proceso de Revisión de instrumentos jurídicos de prestación de servicios relativos al art. 3 del Reglamento del Servicio de Protección Federal.
			12. Proceso de emisión de opiniones a instrumentos jurídicos en materia de Adquisiciones
			13. Procesos Penales
2	Centro de Evaluación y Control de Confianza del SPF	1	1. Proceso de Evaluación y Control de Confianza
3	Dirección General de Administración	4	1. Proceso de Registro de Personal (REP)
			2. Proceso de contratación de bienes y servicios
			3. Proceso de Elaborar y Suscribir Contratos y Convenios
			4. Proceso de Reclutamiento y Selección
4	Dirección General de Profesionalización	9	1. Proceso de Formación Inicial
			2. Proceso de Detección de Necesidades de Capacitación
			3. Proceso de Expediente Electrónico Policial
			4. Proceso de Promoción
			5. Proceso de otorgamiento de Reconocimientos
			6. Proceso de Evaluación del Desempeño
			7. Proceso de Eventos Deportivos
			8. Proceso de Evaluaciones con Fines de Certificación de Competencias Integrantes / Externos
			9. Proceso de Normalización
5	Inspección Interna	4	1. Proceso de atención a quejas, denuncias, peticiones y sugerencias
			2. Proceso de Investigación por incumplimiento a los requisitos de permanencia u obligaciones policiales
			3. Proceso de Módulo del Monitoreo de Conducta de los Integrantes del SPF
			4. Proceso visitas de inspección
6	Dirección General de Servicios de Seguridad	1	1. Proceso de Ingreso a las instalaciones del Servicio de Protección de Federal
	TOTAL		32

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

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.*

De conformidad con lo anterior, las funciones y obligaciones del personal del SPF que trata datos personales se han identificado en dos niveles:

I. A nivel macro, a través de las Políticas de Protección y de Gestión y Tratamiento de Datos Personales del SPF, en las cuales se describen todas las obligaciones que establece la Ley General y los Lineamientos Generales con el área responsable de su cumplimiento, y

II. A nivel de servidor público, a través de los inventarios que se desarrollaron por cada uno de los tratamientos, en los cuales se identificó el personal que realiza el tratamiento, el área al que está adscrito y la finalidad de dicho tratamiento.

Las Políticas de Protección y de Gestión y Tratamiento de Datos Personales del SPF forman parte integral de este documento de seguridad.

Por su parte, el inventario de tratamientos contiene las siguientes columnas, en las cuales se identifican las funciones del personal que interviene en el tratamiento de los datos personales:

Servidores públicos que tienen acceso a la base de datos (15)	*Área de adscripción (16)*	*Finalidad del acceso (17)*
Señalar los puestos de los servidores públicos que tienen acceso a la base de datos del tratamiento correspondiente. Uno por fila.	*Definir unidad administrativa a la que está adscrito el puesto*	*Señalar con qué fines tienen acceso los servidores públicos antes identificados. Uno por fila, según corresponda.*

Asimismo, el Comité de Transparencia es el área responsable de dar a conocer a los servidores públicos del Servicio de Protección Federal, las Políticas de Datos Personales, que se basa en un sistema de gestión, a fin de que el personal conozca sus funciones para el cumplimiento del sistema de gestión y las consecuencias de su incumplimiento.

Adicionalmente, conviene señalar que las funciones y obligaciones del personal que traten datos personales se encuentran definidas en la legislación y normatividad que rige la materia.

III, IV y V. Análisis de Riesgos, Análisis de Brecha y Plan de Trabajo

El artículo 33, fracciones IV, V y VI 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 realización del Análisis de Riesgo, Análisis de Brecha y Plan de Trabajo, en los siguientes términos:

> ***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;*
>
> *[…]*

Como se señaló, 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.

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.*
>
> *Plan de Trabajo*
>
> ***Artículo 62.*** *De conformidad con lo dispuesto en el artículo 33, fracción VI de la Ley General, el responsable deberá elaborar un plan de trabajo que defina las acciones a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de*

brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer.

Lo anterior, considerando los recursos designados; el personal interno y externo en su organización y las fechas compromiso para la implementación de las medidas de seguridad nuevas o faltantes.

Por su parte, el artículo 32, de la Ley General, citado en la fracción V del artículo 60 de los Lineamientos Generales, dispone lo siguiente:

> ***Artículo 32.*** *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.*

A partir de lo dispuesto por los artículos antes citados, el Análisis de Riesgo se lleva a cabo a partir de cuatro fuentes de información:

1. Análisis de riesgos de la infraestructura tecnológica y recursos de software y hardware;
2. Análisis de riesgos de hábitos de seguridad del personal del SPF;
3. Análisis de riesgos a partir de los inventarios de tratamientos de datos personales, y
4. Análisis de riesgos vinculado con el cumplimiento de obligaciones normativas en materia de datos personales.

Los dos primeros análisis se realizan de manera general y aplican transversalmente, ya que el primero refiere a los distintos sistemas o medios en los que se llevan a cabo los diversos tratamientos que realiza el SPF, por lo que los riesgos y controles que se determinen aplican de manera directa a estos medios o sistemas; mientras que el segundo versa sobre los hábitos de seguridad del personal, de manera general y no asociados a un tratamiento en lo particular.

Por su parte, los análisis 3 y 4 se realizan, de manera específica, asociados a cada uno de los tratamientos, y tomando en cuenta sus particularidades.

Los elementos requeridos en los artículos 33, fracción IV, de la Ley General y 60 de los Lineamientos Generales se atienden de la siguiente forma:

Elemento requerido	Fundamento	Fuente	Observaciones
Tomar en cuenta amenazas y vulnerabilidades existentes.	33, fracción IV, de la Ley General.	• Análisis de riesgos de la infraestructura tecnológica y recursos de software y hardware; • Análisis de riesgos de hábitos de seguridad del personal del SPF; • Análisis de riesgos a partir de los inventarios de tratamientos de datos personales, y • Análisis de riesgos vinculado con el cumplimiento de obligaciones normativas en materia de datos personales.	En los cuatro cuestionarios o fuentes se identifican las vulnerabilidades y amenazas específicas.
Tomar en cuenta los recursos involucrados.	33, fracción IV, de la Ley General.	• Análisis de riesgos de la infraestructura tecnológica y recursos de software y hardware, y • Análisis de riesgos a partir de los inventarios de tratamientos de datos personales.	La primera fuente refiere específicamente a los recursos de hardware y software; mientras que en los inventarios se identifican los medios de almacenamiento y obtención de los datos personales y, en su caso, se asocian con sus respectivos riesgos.
Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico.	60, fracción I, de los Lineamientos Generales.	Análisis de riesgos vinculado con el cumplimiento de obligaciones normativas en materia de datos personales.	El cuestionario respectivo refiere a los requerimientos regulatorios. En el caso del SPF, actualmente, no se observan códigos de conducta o mejores prácticas en un sector específico para el tratamiento de datos personales.
El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida.	60, fracción II, de los Lineamientos Generales.	Análisis de riesgos a partir de los inventarios de tratamientos de datos personales.	En el inventario se identifica el tipo de datos tratado y se estructura a partir de su ciclo de vida, lo que es considerado al

Elemento requerido	Fundamento	Fuente	Observaciones
			momento de determinar riesgos y controles de seguridad.
El valor y exposición de los activos involucrados en el tratamiento de los datos personales	60, fracción III, de los Lineamientos Generales.	Análisis de riesgos de hábitos de seguridad del personal del SPF.	A través de este cuestionario se identifican las prácticas que exponen a los datos personales.
Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida.	60, fracción IV, de los Lineamientos Generales.	Ponderación de riesgos.	En la ponderación de riesgos que se realiza en la Fase Cuatro se toma en cuenta las posibles consecuencias de una vulneración para los titulares, para la priorización y determinación del tratamiento del riesgo.
El riesgo inherente a los datos personales tratados.	32, fracción I, de la Ley General.	Análisis de riesgos a partir de los inventarios de tratamientos de datos personales.	En el inventario se identifica el tipo de datos tratado y las finalidades del tratamiento, lo que es considerado al momento de determinar riesgos y controles de seguridad.
La sensibilidad de los datos personales tratados.	32, fracción II, de la Ley General.	Análisis de riesgos a partir de los inventarios de tratamientos de datos personales.	En el inventario se identifica el tipo de datos tratado, lo que es considerado al momento de determinar riesgos y controles de seguridad.
El desarrollo tecnológico.	32, fracción III, de la Ley General.	Análisis de riesgos de la infraestructura tecnológica y recursos de software y hardware.	En el análisis realizado por la DGTI se considera el desarrollo tecnológico, ya que versa sobre dicha materia.
Las posibles consecuencias de una vulneración para los titulares.	32, fracción IV, de la Ley General.	Ponderación de riesgos.	En la ponderación de riesgos que se realiza en la Fase Cuatro se toma en cuenta las posibles consecuencias de una vulneración para los titulares, para la priorización y determinación del tratamiento del riesgo.

Elemento requerido	Fundamento	Fuente	Observaciones
Las transferencias de datos personales que se realicen.	32, fracción V, de la Ley General.	Análisis de riesgos a partir de los inventarios de tratamientos de datos personales.	En el inventario se identifican las transferencias, lo que es considerado al momento de determinar riesgos y controles de seguridad.
El número de titulares.	32, fracción VI, de la Ley General.	Ponderación de riesgos.	En la ponderación de riesgos que se realiza en la Fase Cuatro se toma en cuenta el número de titulares, para la priorización y determinación del tratamiento del riesgo.
Las vulneraciones previas ocurridas en los sistemas de tratamiento.	32, fracción VII, de la Ley General.	Reportes de vulneraciones al Comité de Transparencia.	Una de las obligaciones del Programa de Protección de Datos Personales del SPF es notificar al Comité de Transparencia las vulneraciones ocurridas. A partir de esos reportes, se deberán tomar en cuenta las vulneraciones ocurridas para la definición de los controles y la actualización del documento de seguridad.
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.	32, fracción VIII, de la Ley General.	Ponderación de riesgos.	En la ponderación de riesgos que se realiza en la Fase Cuatro se toma en cuenta 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, para la priorización y determinación del tratamiento del riesgo.

El proceso del Análisis de Riesgos, en lo general, es el siguiente:

Fase Uno. Identificación de posibles riesgos y controles de seguridad preliminares

1. Cada una de las áreas que están a cargo de tratamientos, responden los cuestionarios relativos a los análisis de riesgos de hábitos de seguridad y de cumplimiento de obligaciones normativas.

   Se responde un único cuestionario de cumplimiento de obligaciones por tratamiento, y todo el personal que esté involucrado con el tratamiento debe de responder un cuestionario sobre sus hábitos de seguridad.

2. La Dirección de Tecnologías de la Información y Comunicaciones (DTIC) realiza el análisis de riesgos de la infraestructura y recursos de software y hardware, de acuerdo con la metodología que tiene definida.

3. El área encargada de apoyar en el análisis de riesgos analiza los inventarios y detecta posibles vulnerabilidades y amenazas, y define controles de seguridad preliminares.

4. Una vez que se entregan los cuestionarios respondidos, el área encargada de apoyar en el análisis de riesgos analiza las respuestas y detecta posibles vulnerabilidades y amenazas y define controles de seguridad preliminares.

Fase Dos. Entrevistas y determinación de riesgos y controles de seguridad

5. Una vez que el área encargada de apoyar en el análisis de riesgos tiene identificados las posibles vulnerabilidades y amenazas, así como definidos controles de seguridad preliminares a partir del análisis realizado a los inventarios y los cuestionarios de hábitos de seguridad del personal y cumplimiento de obligaciones, prepara una entrevista con las distintas áreas responsables de los tratamientos, a fin de intercambiar información con relación a los posibles riesgos identificados y los controles de seguridad necesarios para mitigarlos.

   En las entrevistas se debe identificar qué controles de seguridad tiene implementados el área a cargo del tratamiento.

6. A partir de la información obtenida de las distintas entrevistas, el área encargada de apoyar en el análisis de riesgos determinará los riesgos y los controles de seguridad necesarios para mitigarlos.

   No se omite señalar que los riesgos vinculados a la infraestructura tecnológica, software y hardware serán definidos por la DTIC.

Fase Tres. Análisis de Brecha

7. Una vez determinados los riesgos y los controles de seguridad necesarios para mitigarlos, se realiza el análisis de brecha, que consiste en identificar cuáles son los controles que hacen falta implementar a partir de aquéllos definidos como necesarios.

Fase Cuatro. Ponderación de los riesgos y elaboración del Plan de Trabajo

8. Una vez que se han identificado los riesgos y determinado los controles necesarios para mitigarlos, el área que apoya en el análisis de riesgos, la DTIC y el Comité de Transparencia realizarán una ponderación de los riesgos, a fin de determinar cuáles se mitigarán, eliminarán, transferirán o aceptarán, así como priorizar las medidas de seguridad a implementar.

   En la ponderación se deberán tomar en cuenta las posibles consecuencias de una vulneración para los titulares, el número de titulares 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.

   Esta definición se podrá consultar y poner a consideración de las áreas encargadas de los tratamientos.

9. Ya que se ha realizado la ponderación, se elaborará el Plan de Trabajo, en el cual se definirán las acciones a implementar, priorizando las medidas de seguridad más relevantes e inmediatas.

10. En el Plan de Trabajo se deberán identificar los responsables de las acciones, así como las fechas compromiso.

Forman parte integral de este documento de seguridad con el análisis de riesgos de la infraestructura tecnológica y software y hardware, y Plan de Trabajo y la ponderación de riesgos.

VI. Los 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, así como las amenazas y vulneraciones a las que están sujetos los datos personales.

Como se señaló, 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.*

De lo anterior es posible identificar que el monitoreo y revisión de las medidas de seguridad tiene el objetivo de fortalecer, a través de un ciclo de mejor continua, la protección de los datos personales que resguarda este SPF.

A continuación, se desarrollan las acciones de monitoreo y supervisión periódica para las medidas de seguridad del SPF:

Mecanismos de Monitoreo

Para los tratamientos de datos personales del SPF, se consideran los siguientes tipos de monitoreo:

1) **Revisión de cumplimiento de las políticas internas del SPF, relacionadas con el tratamiento de datos personales.** Tiene el objetivo de asegurar que los servidores públicos realicen los tratamientos de datos personales en concordancia con lo dispuesto en la Ley General, los Lineamientos Generales, y demás normatividad que resulte aplicable.

   Para ello, cuando se identifica algún cambio en los instrumentos antes mencionados, se deberán realizar las siguientes actividades:

   a. Revisar y, en su caso, actualizar los procesos involucrados en el tratamiento de datos personales.
   b. Revisar y, en su caso, actualizar los avisos de privacidad, las funciones y obligaciones del personal y los inventarios de datos personales, según corresponda.
   c. Evaluar si hubo cambios en las amenazas, vulnerabilidades o impacto de los riesgos relacionados con las modificaciones a la normativa, para actualizar los análisis de riesgos, análisis de brecha y plan de trabajo.
   d. Revisar y, en su caso, adecuar los sistemas de tratamiento para cumplir con los cambios normativos.

2) **Revisión del riesgo.** Tiene el objetivo de identificar modificaciones a los riesgos identificados en los tratamientos de datos personales, para ello, se implementarán los siguientes monitoreos:

   a. **Monitoreo del entorno físico.** Para la detección continua de amenazas y vulnerabilidades en el entorno físico, se cuenta con: (I) Personal de vigilancia en los accesos al edificio del SPF, (II) Control de acceso del personal con tarjeta de proximidad, (III) Control de acceso a través de bitácoras para visitantes y personal del SPF que olvidó su credencial, y (IV) Control de asistencia a través de huella digital.
   b. **Monitoreo del entorno electrónico.** Para la detección continua de amenazas y vulnerabilidades, la DTIC cuenta con herramientas automatizadas de monitoreo (activo y pasivo), así como con bitácoras de los sistemas informáticos del SPF
   c. **Actualización del plan de trabajo.** Derivado del monitoreo del entorno físico o electrónico, se pueden realizar actualizaciones en el plan de trabajo en caso de que se identifiquen cambios en las amenazas, las vulnerabilidades o el impacto de los riesgos identificados. Estos cambios

se pondrán a consideración del área que apoya en el análisis de riesgos, la DTIC y el Comité de Transparencia.

d. **Revisión de avances del plan de trabajo.** A través de los mecanismos que determine el área que apoya en el análisis de riesgos, la DTIC y el Comité de Transparencia, se hará una revisión de los avances en el plan de trabajo, identificando las acciones, fechas compromiso y, en su caso, las causas por las cuales no se está cumpliendo el plan de trabajo, para hacer los ajustes correspondientes al mismo.

e. **Actualización tecnológica.** Cuando se integren nuevos equipos de cómputo, servidores, aplicaciones o tenga lugar una migración tecnológica, se realizará una actualización del análisis de riesgo.

f. **Vulneraciones a la seguridad de los datos personales.** En caso de identificar un incidente de seguridad que involucre datos personales, el área que apoya en el análisis de riesgos, la DTIC y el Comité de Transparencia se coordinarán para decidir sobre las acciones pertinentes para mitigar dicho incidente.

A continuación, se describen los mecanismos de monitoreo y revisión de este SPF:

Elemento a revisar	Fundamento	Acciones
Los nuevos activos que se incluyan en la gestión de riesgos;	63, fracción I, de los Lineamientos Generales.	1. Revisión de cumplimiento de las políticas internas del SPF, relacionadas con el tratamiento de datos personales.
Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras;	63, fracción II, de los Lineamientos Generales.	1. Revisión de cumplimiento de las políticas internas del SPF, relacionadas con el tratamiento de datos personales. 2. Actualización tecnológica.
Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;	63, fracción III, de los Lineamientos Generales.	1. Revisión de cumplimiento de las políticas internas del SPF, relacionadas con el tratamiento de datos personales. • Monitoreo del entorno físico. • Monitoreo del entorno electrónico.

La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;	63, fracción IV, de los Lineamientos Generales.	1. Revisión de cumplimiento de las políticas internas del SPF, relacionadas con el tratamiento de datos personales. • Monitoreo del entorno físico. • Monitoreo del entorno electrónico.
Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;	63, fracción V, de los Lineamientos Generales.	1. Revisión de cumplimiento de las políticas internas del SPF, relacionadas con el tratamiento de datos personales. • Monitoreo del entorno físico. • Monitoreo del entorno electrónico.
El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo	63, fracción VI, de los Lineamientos Generales.	1. Revisión de cumplimiento de las políticas internas del SPF, relacionadas con el tratamiento de datos personales. • Actualización del plan de trabajo. • Revisión de avances del plan de trabajo.
Los incidentes y vulneraciones de seguridad ocurridas.	63, fracción VII, de los Lineamientos Generales.	1. Revisión de cumplimiento de las políticas internas del SPF, relacionadas con el tratamiento de datos personales. • Vulneraciones a la seguridad de los datos personales.

Mecanismos de supervisión o revisión

Además del monitoreo continuo de las medidas de seguridad, se requiere realizar una supervisión periódica de las medidas de seguridad, a través de auditorías, las cuales pueden ser internas (desarrolladas por el propio SPF) o externas (realizando una contratación o a través de un convenio con un tercero).

Hasta el momento no se han realizado auditorías específicas en materia de protección de datos personales a los tratamientos del SPF.

Así, respecto del programa de auditoría mencionado en el último párrafo del artículo 63 de los Lineamientos Generales, se tiene contemplada la realización de una auditoría en

materia de protección de datos personales, al menos una vez cada dos años. Dicha auditoría se puede llevar a cabo por terceros según la disponibilidad presupuestal, o bien internamente por personal del SPF, conforme lo determine el Comité de Transparencia.

El programa de auditoría será aquél que determine el Comité de Transparencia en el Programa de Protección de Datos Personales del SPF.

Los resultados de las auditorías se considerarán para realizar adecuaciones al análisis de riesgos del SPF y, por lo tanto, al plan de trabajo.

VII. El programa general de capacitación

Con relación al programa de capacitación, la fracción VIII del artículo 33 de la Ley General señala que, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá 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.

Como se señaló, de acuerdo con la fracción VII del artículo 35 de la Ley General, el programa de capacitación forma parte del documento de seguridad.

Por su parte, el artículo 64 de los Lineamientos Generales señala lo siguiente:

> ***Capacitación***
> ***Artículo 64.*** *Para el cumplimiento de lo previsto en el artículo 33, fracción VIII de la Ley General, el responsable deberá diseñar e implementar programas a corto, mediano y largo plazo que tengan por objeto capacitar a los involucrados internos y externos en su organización, considerando sus roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales y el perfil de sus puestos.*
>
> *En el diseño e implementación de los programas de capacitación a que se refiere el párrafo anterior del presente artículo, el responsable deberá tomar en cuenta lo siguiente:*
>
> *I. Los requerimientos y actualizaciones del sistema de gestión;*
> *II. La legislación vigente en materia de protección de datos personales y las mejores prácticas relacionadas con el tratamiento de éstos;*
> *III. Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales, y*

IV. Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad.

Actualización del documento de seguridad

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

En ese sentido, el Comité de Transparencia deberá estar atento a la actualización de alguno de los supuestos antes citado, para, en su caso, actualizar el presente documento de seguridad.

El siguiente cuadro muestra las fechas en que se ha actualizado el documento de seguridad del SPF:

Fecha de actualización
Junio 2023