SISTEMAS DE SUPERVISIÓN Y VIGILANCIA PARA LA PROTECCIÓN DE DATOS PERSONALES EN EL SERVICIO DE ADMINISTRACIÓN TRIBUTARIA

El artículo 24, fracción V, de la **Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados** (LGPDPPSO), establece que entre los mecanismos que se deberán adoptar para cumplir con el principio de responsabilidad, se encuentra el de establecer un sistema de supervisión y vigilancia, incluyendo auditorías, que permita comprobar el cumplimiento de las políticas de protección de datos personales.

Asimismo, el artículo 29, fracción VI, de la LGPDPPSO establece que el documento de seguridad deberá contener, entre otros aspectos, los mecanismos de monitoreo y revisión de las medidas de seguridad.

Al respecto, el artículo 27, fracción VII, de la dicha legislación, dispone que se deberán de monitorear y revisar de manera periódica los aspectos siguientes:

1. Las medidas de seguridad implementadas en la protección de datos personales.

2. Las amenazas y vulneraciones a que están sujetos los tratamientos o sistemas de datos personales.

A. Mecanismo de monitoreo y supervisión en la protección de datos personales

Se ejecutará un mecanismo de monitoreo y supervisión de las medidas de seguridad implementadas en la protección de datos personales, a través de los siguientes ejes:

I. Etapa de Monitoreo. Se requerirá a cada una de las unidades administrativas que reportaron tratamientos de datos personales, a través de sus inventarios, la elaboración de un reporte, en el que deberán precisarse:

	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, que permita protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado.	☐	☐
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 demás normatividad que resulte aplicable, y se ha definido la procedencia de su implementación.	☐	☐
3. Se han definido las funciones, obligaciones y cadena de mando de cada persona servidora pública que trata datos personales, por unidad administrativa.	☐	☐
4. Se ha comunicado a cada persona servidora pública sus funciones, obligaciones y cadena de mando con relación al tratamiento de datos personales que efectúa.	☐	☐
5. El tratamiento de datos se justifica en sus atribuciones previstas en la normativa que regula su actuación.	☐	☐

6. En el tratamiento de datos personales se cumplen con los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad.	☐	☐
7. Se han establecido los controles o mecanismos que tengan por objeto prevenir la difusión de los datos personales a personas no autorizadas o legitimadas. Considerando lo siguiente: • El listado de personas servidoras públicas que intervienen en el tratamiento de datos se encuentra actualizado;	☐	☐
• Me aseguro de que las personas servidoras públicas conozcan sus obligaciones con relación a la protección de datos personales, y	☐	☐
• Cumplo con las medidas de seguridad que corresponden al tratamiento de datos personales que realizó.	☐	☐
8. Se mantienen exactos, completos, correctos y actualizados los datos personales. Considerando lo siguiente: • Las fuentes de obtención de los datos personales son confiables y las adecuadas, y	☐	☐
• Cuando tengo conocimiento, a través de una fuente autorizada o confiable del cambio en el registro de algún dato personal, lo actualizo o corrijo en el archivo o base de datos que corresponda.	☐	☐
9. 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 personas servidoras públicas 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.	☐	☐
10. 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;	☐	☐
• La cancelación, supresión o destrucción de los datos personales, y	☐	☐
• Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico.	☐	☐

11. Se ha realizado el análisis de riesgo, considerando lo siguiente: 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.	☐	☐
12. 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.	☐	☐
13. Se ha elaborado el aviso de privacidad, tomando en cuenta lo siguiente: • La finalidad es concreta, lícita, explícita y legítima;	☐	☐
• Se informa la finalidad de manera clara en el aviso de privacidad;	☐	☐
• El tratamiento se limita para las finalidades informadas en el aviso de privacidad;	☐	☐
• Respeto la finalidad por la que recabé los datos de la persona titular, y	☐	☐
• Me cercioro de que los datos personales se encuentran protegidos	☐	☐
14. Se recaban los datos personales, acreditando lo siguiente: • Respeto la finalidad por la que recabé los datos de la persona titular;	☐	☐
• Me cercioro de que los datos personales se encuentran protegidos;	☐	☐
• El tratamiento actualiza alguno de los supuestos previstos en el artículo 14 de la LGPDPPSO, y	☐	☐
• En el procedimiento correspondiente se prevé la obtención del consentimiento.	☐	☐
15. Se monitorea y revisa 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.	☐	☐

I. Etapa de Supervisión. Se analizarán los reportes de las unidades administrativas, verificando aquellos puntos en los que se hubiera reportado "No" como respuesta y se emitirá un dictamen o ficha técnica en el que se plasmarán las recomendaciones o requerimientos que se consideren pertinentes en materia de seguridad, con la finalidad de que las unidades administrativas las atiendan y remitan las evidencias de su cumplimiento.

B. Mecanismos de actuación ante vulneraciones a la seguridad de los datos personales

El artículo 27, fracción VII, de la LGPDPPSO, 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.**

Por ello, se deberá monitorear y revisar de manera periódica las medidas de seguridad, así como las amenazas y vulneraciones a las que están sujetos los datos personales.

Adicionalmente, también resulta oportuno 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 podría 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. La unidad administrativa que advirtió de la alerta de seguridad deberá enviar un reporte a la Unidad de Transparencia, en un plazo no mayor a 72 horas, en el que deberá informar:

   - Circunstancias de modo, tiempo y lugar en que se detectó la amenaza.
   - Sistema de Tratamiento de Datos Personales 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. La Unidad de Transparencia registrará la alerta de seguridad y la remitirá a la Administración General competente, a través de su enlace en materia de datos personales, quien analizará el impacto de la amenaza y, de ser posible, determinará una estrategia de prevención, con la finalidad de evitar que la alerta de seguridad pueda desencadenarse.

C. Mecanismos de auditoría en materia de datos personales

Entre los mecanismos que se deben adoptar para cumplir con el principio de responsabilidad el artículo 24, fracción V, de la LGPDPPSO, establece que se deberá mantener un sistema de supervisión y vigilancia, incluyendo auditorías, que permita comprobar el cumplimiento de las políticas de datos personales.

Por tanto, resulta necesario establecer un mecanismo que permita dar cumplimiento a las disposiciones antes citadas, mismo que se desarrolla de la siguiente manera:

Las auditorías en materia de datos personales tendrán las finalidades siguientes:

- ✓ Verificar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados para el cumplimiento de las disposiciones previstas en la LGPDPPSO.

Es importante señalar que las auditorías que se realicen tendrán por objeto analizar el cumplimiento de los deberes y principios en los tratamientos de los datos personales que fueron documentados a través de los inventarios por cada una de las unidades administrativas, por lo que, la Unidad de Transparencia propondrá al Comité de Transparencia la programación por inventario y, el deber o principio que deberá ser objeto de la auditoría.

Lo anterior, permitirá identificar de forma ordenada las acciones y mejoras que habrán de implementarse para el adecuado manejo y protección de los datos personales.