SISTEMA DE SUPERVISIÓN Y VIGILANCIA PARA LA PROTECCIÓN DE DATOS PERSONALES EN LA SECRETARIA DE SEGURIDAD PÚBLICA

Objetivo General

El sistema de supervisión y vigilancia para la protección de datos personales es una herramienta que el servidor público nombrado como **ÓRGANO DE CONTROL** tiene por objeto verificar que los procedimientos que se implementan, garanticen la Protección a los Datos Personales de conformidad a lo establecido en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

I. Mecanismos de supervisión, vigilancia, monitoreo.

El artículo 30, fracción V, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Ley General), 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.**

En ese sentido, **el artículo 35, fracción VI, de la Ley General** 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 numeral 33, fracción VII, de 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.**

Etapa de monitoreo: Registrar los controles de seguridad instaurados en determinado Tratamiento.

- **Controles de acceso**
- **Vigilancia física**
- **Registro de actividades en rol de servicio**

Etapa de Supervisión: Análisis y valoración de la efectividad de los controles de seguridad instaurados.

- **Auditorias de seguridad (respaldo físico y digital contenido en carpetas contenedoras que van a un repositorio central de un servidor)**

- **Mejora continua y Capacitación**
- **Encriptación de datos y respaldo**
- **Actualizaciones de seguridad (actualización de contraseñas de forma periódica con copia a supervisión del requerimiento para el respaldo)**

Al respecto, el artículo 63 de los Lineamientos Generales, dispone que se deberá monitorear continuamente lo siguiente:

1. Los nuevos activos que se incluyan en la gestión de riesgos (**definición del INAI: activo es todo elemento de valor involucrado en el tratamiento de datos personales, como pueden ser una base de datos, el conocimiento de los procesos, el personal, el hardware, el software, los archivos o los documentos en papel).**

De esta manera, se pueden identificar ***dos tipos de activos:***

• **Activos de información**
- Información relativa a los datos personales.
- Información de procesos en los que interviene el flujo de datos personales, actividades involucradas en el tratamiento de los mismos.

• **Activos de apoyo**, en los cuales residen los activos de información, como son:
- Hardware.
- Software
-Infraestructura

Mismos que se deberán de mantener actualizados, así como los medios de almacenamiento.

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. **(del entorno y de origen natural)**

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 ocurridas.

Además de lo expuesto, el artículo referido estipula que el responsable deberá contar con un programa de auditoría para monitorear y revisar la eficacia y eficiencia del sistema de gestión.

II. Revisión, alertas, vulneraciones

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

Ante una vulneración en la seguridad de los datos personales, los artículos 37 a 41 de la Ley General, establecen las obligaciones siguientes:

1. Analizar las causas por las cuales se presentó e implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales a efecto de evitar que la vulneración se repita.

2. Inscribir la vulneración en la bitácora de las vulneraciones.

3. Informar sin dilación alguna a la persona titular y al Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (INAI), las vulneraciones que afecten de forma significativa derechos patrimoniales o morales, a fin de que las y los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos.

Con referencia al artículo 38 de la LGPDPPSO Se entenderá por vulneración lo siguiente:

I. La pérdida o destrucción no autorizada;
II. El robo, extravío o copia no autorizada;
III. El uso, acceso o tratamiento no autorizado, o
IV. El daño, la alteración o modificación no autorizada

Para su análisis el responsable deberá de tomar en cuenta las **Recomendaciones Para Reconocer Las Principales Amenazas A Los Datos Personales** publicado por el INAI en su edición de abril 2021.

III.. Auditoria

Las auditorías deberán incluir la revisión del cumplimiento de las obligaciones que tiene el Comité de Transparencia, la aplicación de las presentes Políticas y Lineamientos; evaluar la conformidad con las mismas

El Consejo de la Judicatura Federal elaboró el Mecanismo de Auditoria en materia de Datos Personal, tomándolo como referencia, dicho mecanismo cuenta con las finalidad y objetivo siguiente:

- Determinar que los tratamientos de datos personales se encuentren apegados a la normativa aplicable.
- Supervisar la adopción y cumplimiento de las políticas, procedimientos y mecanismos determinados en el Sistema de Gestión y el Documento de Seguridad.
- Verificar la eficiencia de las medidas de seguridad físicas, administrativas y técnicas instauradas.
- Validar el avance de los objetivos planteados en el Plan de Trabajo.
- Prevenir la materialización de vulneraciones a la seguridad de los datos personales.
- Promover la implementación de mejoras en el tratamiento de los datos personales, que permitan elevar su grado de protección.