MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

El artículo 30, fracción V de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 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 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 artículo 33, fracción VII de la Ley General, 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

El artículo 63 de los Lineamientos Generales de protección de datos personales para el sector público establece que 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 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 auditoría, interno y/o externo, para monitorear y revisar la eficacia y eficiencia del sistema de gestión.

En ese sentido, el INAI desarrollará el cumplimiento de dicha obligación a través de los siguientes mecanismos:

A. Mecanismo de monitoreo y supervisión

La Unidad de Transparencia será la encargada de ejecutar el 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. La Unidad de Transparencia requerirá a cada una de las áreas que reportaron tratamientos de datos personales, a través de sus inventarios, el llenado de los formatos adjuntos al presente documento.
II. Etapa de Supervisión. La Unidad de Transparencia analizará los reportes de las áreas, y emitirá un documento 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. Mecanismos de actuación ante vulneraciones a la seguridad de los datos personales

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 de Protección de Datos Personales para el Sector Publico, 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, la Unidad de Transparencia 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, para lo cual se podrá auxiliar de todas las unidades administrativas que estime necesarias.

Adicionalmente, 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 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, 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. La Unidad de Transparencia registrará la alerta de seguridad y analizará el impacto de la amenaza y, de ser posible, determinará una estrategia de prevención, para lo cual, podrá apoyarse de las áreas técnicas y normativas de la SENER, con la finalidad de evitar que la alerta de seguridad pueda desencadenarse.

C. Mecanismos de supervisión y vigilancia en materia de datos personales

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.