Sistema de Supervisión y Vigilancia de la Secretaría de Infraestructura, Comunicaciones y Transportes.

I. Introducción.

El artículo 29 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) establece que se deberán implementar mecanismos para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en la Ley en la materia.

Asimismo, de conformidad con lo establecido en el artículo 30, fracción V, de la LGPDPPSO, entre los mecanismos que se deberán adoptar para cumplir con el principio de responsabilidad, se encuentra el sistema de supervisión y vigilancia, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.

Por su parte, el artículo 33, fracción VII, de la LGPDPPSO establece que, para mantener las medidas de seguridad para la protección de los datos personales, se deberán monitorear y revisar de manera periódica las medidas de seguridad que se tengan implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales.

Correlativamente, el artículo 63 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales) 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.

A efecto de cumplir con lo anterior, se 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 la Secretaría 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 ocurridos.

Aunado a lo anterior, se deberá contar con un programa de auditoría para monitorear y revisar la eficacia y eficiencia del sistema de gestión.

Con base en lo anterior, la Secretaría de Infraestructura, Comunicaciones y Transportes (SICT) da cumplimiento a las obligaciones mencionadas a través de los siguientes mecanismos:

II. Mecanismo de monitoreo y supervisión.

La Unidad de Transparencia, a través de la persona designada como Oficial de Protección de Datos Personales, será la encargada de ejecutar el mecanismo de monitoreo y supervisión de las medidas de seguridad implementadas en la protección de datos personales que tratan las unidades administrativas de la SICT, considerando lo siguiente:

- **Etapa de Monitoreo**. La Unidad de Transparencia requerirá a cada una de las unidades administrativas que reportaron tratamientos de datos personales, a través de sus inventarios de datos personales, la elaboración de un informe que considere lo siguiente:

a) Manifestación de que todo tratamiento de datos personales que se efectúe deberá estar debidamente justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera.

b) Observancia de los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales.

c) Existencia de Avisos de Privacidad, en sus modalidades integral y simplificado, entendido como el documento a disposición del titular de forma física, electrónica o en cualquier otro formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de éstos.

d) Existencia de medidas de seguridad administrativas, técnicas y físicas necesarias para la protección de datos personales.

e) Identificación de funciones, obligaciones y cadena de mando de cada persona servidora púbica que trata datos personales.

f) Existencia de inventario de datos personales que contemple catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales; finalidades del tratamiento; tipos de datos personales indicando si son sensibles o no; catálogo de formatos de almacenamiento, descripción general de la ubicación física y electrónica de los datos personales; personas servidoras públicas con acceso a los sistemas de tratamiento y, en su caso, nombre o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable.

g) Existencia de análisis de riesgo, 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, y un análisis de brecha comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable.

h) Cumplimiento al Programa de Capacitación en materia de protección de datos personales por parte de las personas servidoras públicas.

i) Supervisar que los mecanismos que se lleven a cabo para la entrega de la información aseguren que los datos personales únicamente se entreguen al titular o, en su caso, al representante legal debidamente acreditado. Asimismo, se informe al titular el monto de los costos a cubrir por la reproducción y envío de los datos personales, con base en lo establecido en las disposiciones normativas aplicables.

❖ **Etapa de Supervisión.**

La Unidad de Transparencia, a través de la persona designada como Oficial de Protección de Datos Personales, analizará los reportes de las unidades administrativas, verificando aquellos puntos en los que se hubiera reportado "No" como respuesta y se emitirá un proyecto de dictamen en el que se plasmarán las recomendaciones o requerimientos que se consideren pertinentes en materia de seguridad, con la finalidad de que sea aprobado por el Comité de Transparencia, en su carácter de autoridad máxima en materia de protección de datos personales, y se instruya a las unidades administrativas su cumplimiento.

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

El artículo 33, fracción VII, de la LGPDPPSO dispone que, para establecer y mantener las medidas de seguridad para la protección de los datos personales, los sujetos obligados deberán 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.

El artículo 63, fracción VII, de los Lineamientos Generales, entre otras disposiciones señala 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, a través de la persona designada como Oficial de Protección de Datos Personales, en coordinación con las unidades responsables, 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.

Con el fin de contar con un mecanismo que permita monitorear las alertas de seguridad de los datos personales, como posibles incidentes de seguridad, la Unidad de Transparencia en coordinación con las unidades administrativas responsables de los sistemas de tratamiento de datos personales llevarán a cabo 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 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, a través de la persona designada como Oficial de Protección de Datos Personales, registrará la alerta de seguridad y analizará, en coordinación con la Dirección General de Tecnologías de Información y Comunicaciones, 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 SICT, con la finalidad de evitar que la alerta de seguridad pueda desencadenarse.

IV. Mecanismos de auditoría en materia de datos personales.

El artículo 63 de los Lineamientos Generales dispone que, además del monitoreo y supervisión periódica de las medidas de seguridad, se deberá contar con un programa de auditoría para revisar la eficacia y eficiencia del sistema de gestión de datos personales.

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 y los Lineamientos Generales.

V. Mecanismos de cumplimiento.

La Unidad de Transparencia notificará a la unidad administrativa responsable del sistema de tratamiento de datos personales los resultados de la Auditoría para su conocimiento y atención correspondiente.

La Unidad de Transparencia notificará al Comité de Transparencia los resultados de la auditoría y la atención brindada por la unidad administrativa responsable del sistema de tratamiento de datos personales.