MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD DEL TRATAMIENTO DE LOS DATOS PERSONALES DE AICM Y SACM

Capitán Carlos León s/n Colonia Peñón de los Baños Alcaldía Venustiano Carranza C.P. 15520, Ciudad de México. Teléfono: 01 (55) 2482-2400 www.gob.mx/aicm

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Ley), en el artículo 30, fracción V, establece que entre los mecanismos que se deberán adoptar para cumplir con el **principio de responsabilidad,** está el establecer un **sistema de supervisión y vigilancia**, incluyendo auditorías, que permita comprobar el cumplimiento de las políticas de protección de datos personales.

El artículo 35, fracción VI, de la Ley establece que el Documento de seguridad deberá contener, entre otros aspectos, los mecanismos de monitoreo y revisión de las medidas de seguridad.

El artículo 33, fracción VII de la Ley 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 Público, 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 lo siguiente:

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

La Unidad de Transparencia será la encargada de implementar el mecanismo de monitoreo y supervisión de las medidas de seguridad para la protección de datos personales, a través de los siguientes ejes:

I. **Etapa de Monitoreo.** Se solicitará a cada una de las áreas que reportaron tratamientos de datos personales, la elaboración de un reporte, en el que deberán precisarse:

	Sí	No
1. Se han definido, se establecen y mantienen las medidas de seguridad administrativas, técnicas y físicas necesarias para la protección de los datos personales.	☐	☐
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 considera medidas de seguridad específicas o adicionales a las previstas en la Ley y los Lineamientos Generales, y se ha definido la procedencia de su implementación.	☐	☐
3. Se han definido las funciones, obligaciones y cadena de mando de cada servidor público que trata datos personales, por unidad administrativa.	☐	☐
4. Se ha comunicado a cada servidor público sus funciones, obligaciones y cadena de mando con relación al tratamiento de datos personales que efectúa.	☐	☐
5. 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;	☐	☐

Capitán Carlos León s/n Colonia Peñón de los Baños Alcaldía Venustiano Carranza C.P. 15520, Ciudad de México. Teléfono: 01 (55) 2482-2400 www.gob.mx/aicm

	Sí	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 servidores públicos 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.		
6. 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, y • La cancelación, supresión o destrucción de los datos personales.	☐	☐
7. Se ha realizado el análisis de riesgo, considerando lo siguiente: • Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico; • 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;	☐	☐

Capitán Carlos León s/n Colonia Peñón de los Baños Alcaldía Venustiano Carranza C.P. 15520, Ciudad de México. Teléfono: 01 (55) 2482-2400 www.gob.mx/aicm

	Sí	No
• 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.		
8. 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.	☐	☐
9. 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.	☐	☐

II. **Etapa de Supervisión.** Se analizarán los reportes de las áreas, 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 de la información, con la finalidad de que las áreas las atiendan y remitan las evidencias de su cumplimiento.

Capitán Carlos León s/n Colonia Peñón de los Baños Alcaldía Venustiano Carranza C.P. 15520, Ciudad de México. Teléfono: 01 (55) 2482-2400 www.gob.mx/aicm

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

Ante una vulneración a la seguridad de los datos personales se deberá proceder de conformidad con lo establecido en el documento denominado "**Guía para registrar y reportar vulneraciones de datos personales Aeropuerto Internacional de la Ciudad de México, S.A. de C.V.**" el cual contemplan las actividades que deben realizar cuando se materialice una vulneración de seguridad en cualquier fase del tratamiento de datos personales.

Asimismo, como mecanismo para monitorear los posibles incidentes de seguridad, se deberán llevar acabo 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 Subdirección de Sistemas y 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 analizará el impacto de la amenaza y, de ser posible, determinará una estrategia de prevención, para lo cual, podrá apoyarse de la Subdirección de Sistemas, con la finalidad de evitar que la alerta de seguridad pueda desencadenarse.

Capitán Carlos León s/n Colonia Peñón de los Baños Alcaldía Venustiano Carranza C.P. 15520, Ciudad de México. Teléfono: 01 (55) 2482-2400 www.gob.mx/aicm

C. Mecanismos de auditoría en materia de datos personales

Con la finalidad de cumplir con el **principio de responsabilidad** el artículo 30, fracción V, de la Ley General de Datos Personales en Posesión de Sujetos Obligados, el cual establece que se deberá mantener un sistema de supervisión y vigilancia, incluyendo auditorías, que permita comprobar el cumplimiento de las políticas de datos personales.

Asimismo, en el artículo 63 de los Lineamientos precisa 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.

Al respecto, 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 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.

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, con la finalidad de identificar de forma ordenada las acciones y mejoras que habrán de implementarse para el adecuado manejo y protección de los datos personales.

Capitán Carlos León s/n Colonia Peñón de los Baños Alcaldía Venustiano Carranza C.P. 15520, Ciudad de México. Teléfono: 01 (55) 2482-2400 www.gob.mx/aicm