SISTEMA DE SUPERVISIÓN Y VIGILANCIA

MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Fiscalía General de la República

Unidad Especializada en Transparencia y Apertura Gubernamental

DISPOSICIONES GENERALES

INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO.

Para establecer y mantener las medidas de seguridad para la protección de los datos personales, las unidades administrativas de la Fiscalía General de la República deberán elaborar un Inventario de los Sistemas de Datos Personales y de los Sistemas de Tratamiento.

FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATEN DATOS PERSONALES.

Para establecer y mantener las medidas de seguridad para la protección de los Sistemas de Datos Personales, las unidades administrativas de la Fiscalía General de la Republica deberán definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales.

ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA.

Con el objeto de establecer y mantener las medidas de seguridad para la protección de los Sistemas de Datos Personales, las unidades administrativas de la Fiscalía General de la República, deberán realizar un análisis de riesgo de los datos personales, y un análisis de brecha comparando las medidas de seguridad existentes contra las faltantes de cada uno de los Sistemas de Datos Personales; 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.

PLAN DE TRABAJO

Formato del Plan de Trabajo que deberán establecer todas las unidades administrativas que mantienen y operan Sistemas de Datos Personales.

MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

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, lo anterior de conformidad con el artículo 30, fracción V, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO).

Asimismo, se establece que el documento de seguridad deberá contener, entre otros aspectos, los mecanismos de monitoreo y revisión de las medidas de seguridad, acorde con lo dispuesto en el artículo 35, fracción VI, de la LGPDPPSO.

Al respecto, el artículo 33, fracción VII, de la LGPDPPSO, dispone que se deberán de monitorear y revisar de manera periódica los aspectos siguientes:

- Las medidas de seguridad implementadas en la protección de datos personales.
- Las amenazas y vulneraciones a que están sujetos los tratamientos o sistemas de datos personales

En ese sentido, 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, la persona responsable deberá monitorear continuamente los siguientes aspectos:

- 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 del sujeto obligado 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.
- Los incidentes y vulneraciones de seguridad ocurridos.

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

MECANISMO DE MONITOREO Y SUPERVISIÓN

Se debe llevar a cabo el mecanismo de monitoreo y supervisión de las medidas de seguridad implementadas en la protección de datos personales, a través de las siguientes vertientes:

ETAPA DE MONITOREO

INDICACIÓN	SI	NO
Se tienen definidas, establecidas y mantienen las medidas de seguridad administrativas, técnicas y físicas necesarias para la protección de los datos personales.	☐	☐
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 los Lineamientos Generales.	☐	☐
Se han definido las funciones, obligaciones y cadena de mando de cada servidor público que trata datos personales, por unidad administrativa.	☐	☐
Se ha comunicado a cada servidor público sus funciones, obligaciones y cadena de mando con relación al tratamiento de datos personales que efectúa.	☐	☐
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 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.	☐	☐
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.	☐	☐
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 con 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.		
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.	☐	☐
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.	☐	☐

MECANISMOS DE ACTUACIÓN ANTE VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES

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 virtud de lo dispuesto en el artículo 33, fracción VII de la LGPDPPSO

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.

En virtud de lo anterior, las unidades administrativas deberán 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, 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:

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.

MECANISMOS DE AUDITORÍA 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, incluyendo auditorías, que permita comprobar el cumplimiento de las políticas de datos personales.

El artículo 63 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público (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.

Las auditorías pueden ser:

- Internas
- Externas, cuando exista el presupuesto para ello y la importancia del caso lo amerite, o
- Voluntarias, realizadas a través del INAI según el artículo 151 de la LGPDPPSO, cuando sea con relación a un tratamiento específico y no a todo el sistema de gestión de los 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 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 que fueron documentados a través de los inventarios por cada una de las unidades administrativas.

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.

CANCELACIÓN DE DATOS PERSONALES.

Para proceder a la baja o destrucción documental de soportes físicos que contienen datos personales, se observarán las disposiciones en materia de archivos que emita Fiscalía General de la República.

Todo soporte electrónico que sea dado de baja (ya sea por obsoleto, sustitución, ejercicio del derecho de cancelación o alguna otra causa) deberá pasar por un proceso de preparación final antes de ser desechado. El personal encargado de los Sistemas de Datos Personales vigilará que se sigan los procedimientos y se utilicen los mecanismos para asegurar la destrucción de soportes electrónicos que contengan datos personales.