



**GOBIERNO DE
MÉXICO**



CONACYT
Consejo Nacional de Ciencia y Tecnología



Mecanismos de monitoreo y
revisión de las medidas de
seguridad

CENTRO DE INVESTIGACIÓN EN MATEMÁTICAS, A.C. (CIMAT)

MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

2022





**GOBIERNO DE
MÉXICO**



CONACYT
Consejo Nacional de Ciencia y Tecnología



INTRODUCCIÓN

Toda vez que 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, incluyendo auditorías, que permita comprobar el cumplimiento de las políticas de protección de datos personales.

Por su parte, 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.

El artículo 33, fracción VII, de la Ley General, 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 mismo sentido, el artículo 63 de los lineamientos establece que el CIMAT en su calidad de 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, se 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, y
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 Centro de Investigación en Matemáticas, A.C. desarrollará el cumplimiento de dicha obligación a través de los siguientes mecanismos:



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:

Etapa de Monitoreo. La Unidad de Transparencia requerirá a cada una de las Áreas Competentes que reportaron tratamientos de datos personales, a través de sus inventarios, la elaboración de un reporte, en el que deberán precisarse:

Table with 3 columns: Question, Sí, No. Contains 6 rows of monitoring questions regarding data security measures.



<ul style="list-style-type: none"> • 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. 		
<p>7. Se ha realizado el análisis de riesgo, considerando lo siguiente:</p> <ul style="list-style-type: none"> • 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; • 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. 	□	□
<p>8. Se ha realizado el análisis de brecha, tomando en cuenta lo siguiente:</p> <ul style="list-style-type: none"> • Las medidas de seguridad existentes y efectivas; • Las medidas de seguridad faltantes, y • La existencia de nuevas medidas de seguridad que pudieran reemplazar a uno o más controles implementados actualmente. 	□	□
<p>10. 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:</p> <ul style="list-style-type: none"> • 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.

Etapas de Supervisión. La Unidad de Transparencia analizará 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, con la finalidad de que las áreas las atiendan y remitan las evidencias de su cumplimiento.

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 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 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 las mismas áreas competentes.

En el documento **“Guía para registrar y reportar vulneraciones de datos personales”** se concentran las actividades que deben realizarse cuando se materialice una **vulneración de seguridad** en cualquier fase del tratamiento de datos personales.

Adicionalmente, también 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:



GOBIERNO DE
MÉXICO



CONACYT
Consejo Nacional de Ciencia y Tecnología



- 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 del Instituto, con la finalidad de evitar que la alerta de seguridad pueda desencadenarse.

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. Por tanto, 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 que fueron documentados a través de los



**GOBIERNO DE
MÉXICO**



CONACYT
Consejo Nacional de Ciencia y Tecnología



inventarios por cada una de las áreas, por lo que, la Unidad de Transparencia propondrá al Comité de Transparencia la programación por inventario y, el deber o principio que deberá ser objeto de la auditoría.

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.



CIMAT