



## SISTEMAS DE SUPERVISION Y VIGILANCIA

La normatividad establecida los Lineamientos Generales para la Protección de Datos Personales y la Ley General de Protección de Datos Personales en Posesión de los sujetos obligados, establece la obligatoriedad para las Dependencias y entidades de la Administración Pública, de monitorear y revisar las medidas de seguridad implementadas y vigilar la presentación de amenazas y vulneraciones a que están sujetos los tratamiento de datos personales.

Para dar cumplimiento a estos preceptos, el responsable de datos personales debe monitorear:

1. Actualizaciones tecnológicas para la protección de datos.
2. Revisar su matriz de riesgos y realización de su valoración.
3. Variaciones y consecuencias de amenazas, vulnerabilidades y riesgos integrales, que sean producto en un nivel alto de riesgo.
4. Los incidentes y vulneraciones de seguridad ocurridos.

Por lo anterior, el Centro dará cumplimiento de dichas obligaciones estableciendo lo siguientes procesos:

### I.- Monitoreo

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, considerando la siguiente evaluación:

	Sí	No
1. Se establecen y mantienen las medidas de seguridad administrativas, técnicas y físicas necesarias para la protección de los datos personales.	<input type="checkbox"/>	<input type="checkbox"/>
2. Se consulta el marco normativo que regula en lo particular el tratamiento de datos personales, con la finalidad de que se cumpla la aplicación de la Ley sus Lineamientos.	<input type="checkbox"/>	<input type="checkbox"/>
3. Se han definido las funciones, obligaciones y cadena de mando de cada servidor público que trata datos personales, por unidad administrativa.	<input type="checkbox"/>	<input type="checkbox"/>
4. Se comunica al responsable de datos personales sus funciones, obligaciones y cadena de mando con relación al tratamiento de datos personales que efectúa.	<input type="checkbox"/>	<input type="checkbox"/>
5. Se elabora el inventario de datos personales con los siguientes elementos: <ul style="list-style-type: none"> <li>• Las finalidades de cada tratamiento de datos personales;</li> <li>• El catálogo de los tipos de datos personales que se traten,</li> <li>• El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales;</li> <li>• La lista de servidores públicos que tienen acceso a los sistemas de tratamiento;</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>



<ul style="list-style-type: none"> <li>En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que las justifican.</li> </ul>		
<p>6. En el inventario de datos personales se tomó en cuenta el ciclo de vida de los datos personales, conforme a lo siguiente:</p> <ul style="list-style-type: none"> <li>La obtención de los datos personales;</li> <li>El almacenamiento de los datos personales;</li> <li>La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen;</li> <li>El bloqueo de los datos personales, en su caso, y</li> <li>La cancelación, supresión o destrucción de los datos personales.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>
<p>7. Se realiza análisis de riesgo, considerando lo siguiente:</p> <ul style="list-style-type: none"> <li>Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico;</li> <li>El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida;</li> <li>Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida;</li> <li>La sensibilidad de los datos personales tratados;</li> <li>El desarrollo tecnológico;</li> <li>Las transferencias de datos personales que se realicen;</li> <li>Las vulneraciones previas ocurridas en los sistemas de tratamiento, y</li> <li>El riesgo pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>
<p>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:</p>	<input type="checkbox"/>	<input type="checkbox"/>

## II.- Supervisión

La Unidad de Transparencia revisará los reportes de las áreas, dando énfasis a los puntos cuya respuesta haya sido negativa y se emitirá las recomendaciones que se consideren necesarios en materia de seguridad.

## III.- Actuación ante vulneraciones a la seguridad 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 este sentido 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.



GOBIERNO DE  
MÉXICO



CONAHCYT  
CONSEJO NACIONAL DE HUMANIDADES  
CIENCIAS Y TECNOLOGÍAS



### Auditoría en materia de datos personales

Se deberá mantener un sistema de supervisión y vigilancia, incluyendo auditorías, que permita comprobar el cumplimiento de las políticas de datos personales, por lo que se realizará auditoría en materia de datos personales con la finalidad de verificar la adecuación y eficiencia de los controles y procesos implementados para el cumplimiento de las disposiciones previstas en la normatividad en la materia.

La realización de los procesos descritos, propiciará la ejecución de las acciones y mejoras que tengan que implementarse para el correcto manejo y protección de los datos personales del CIMAV.