MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

CONAHCYT 2024

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, establece en su articulo 30, fracción V, 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.

Asimismo, el artículo 33, fracción VII, de la Ley General, dispone que se deberán de monitorear y revisar de manera periódica los aspectos siguientes:

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

En ese mismo sentido el articulo 35, fracción VI, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados establece que el documento de seguridad deberá contener, los mecanismos de monitoreo y revisión de las medidas de seguridad.

Por otro lado, los Lineamientos Generales de protección de datos personales para el sector público, en el articulo 63 señalan que es obligación del responsable 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 y contar con un programa de auditoría, interno y/o externo, para monitorear y revisar la eficacia y eficiencia del sistema de gestión.

- 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.

I. MONITOREO Y SUPERVISIÓN

La Unidad de Transparencia verificará el mecanismo de monitoreo y supervisión de las medidas de seguridad implementadas en la protección de datos personales.

Etapa de Monitoreo. Se requerirá a cada una de las Unidades Administrativas que reportaron tratamientos de datos personales, a través de sus inventarios, que precisen los aspectos siguientes:

1. Políticas y Procedimientos		
Actividad	**Cumplimiento**	
1. ¿Existen políticas escritas y aprobadas sobre la seguridad de los datos personales?	**Si**	**No**
2. ¿Se revisan y actualizan estas políticas de manera regular?		
3. ¿Las políticas incluyen responsabilidades específicas para la gestión de datos personales?		
4.- El personal que interviene en los procesos ¿conoce las políticas aprobadas?		
2. Medidas de Seguridad Implementadas		
1. ¿Se han implementado medidas de seguridad físicas, técnicas y administrativas adecuadas para proteger los datos personales?		
2. ¿Se realiza una evaluación periódica de la eficacia de estas medidas de seguridad?		
3. ¿Existen procedimientos para actualizar las medidas de seguridad cuando se identifican deficiencias?		
3. Gestión de Riesgos		
1. ¿Se realiza un análisis de riesgos de manera regular para identificar y evaluar riesgos potenciales para la seguridad de los datos personales?		

2. ¿El análisis de riesgos incluye consideraciones sobre amenazas internas y externas?		
3. ¿Se cuenta con un plan de acción para mitigar los riesgos identificados?		
4. Capacitación y Conciencia		
1. ¿Se ofrece capacitación regular sobre protección de datos personales a los empleados?		
2. ¿Se evalúa la eficacia de la capacitación proporcionada?		
3. ¿El personal conoce el procedimiento cómo reportar incidentes de seguridad de datos?		
5. Auditorías y Monitoreo		
1. ¿Se llevan a cabo auditorías internas o externas de las prácticas de seguridad de datos?		
2.-¿Se cuenta con un calendario de auditorías?		
3. ¿Se monitorean las actividades de tratamiento de datos personales para detectar y responder a incidentes de seguridad?		
4. ¿Existen registros de acceso que permitan revisar quién ha accedido a los datos personales?		
6. Gestión de Incidentes		
1. ¿Existe un procedimiento formal para gestionar y responder a los incidentes de seguridad de datos?		
2. ¿Se llevan registros detallados de todos los incidentes de seguridad?		
3. ¿Existe un procedimiento formal para gestionar y responder a los incidentes de seguridad de datos?		
7. Revisión de Terceros		
1. ¿Se revisan y evalúan las prácticas de seguridad de los terceros que manejan datos personales en nombre de la Institución?		
2. ¿Existen acuerdos que obliguen a los terceros a cumplir con las normativas de protección de datos personales?		

8. Cumplimiento Legal		
1. ¿Se revisan las prácticas de protección de datos personales para asegurar que están en conformidad con la Ley General de Protección de Datos Personales y otras regulaciones relevantes?		
2. ¿Se documentan todas las actividades de cumplimiento?		

SUPERVISIÓN

La Unidad de Transparencia verificara los reportes de las áreas, revisando aquellos puntos en los que se hubiera reportado "No" como respuesta y emitirá las recomendaciones que se consideren pertinentes en materia de seguridad, con la finalidad de que las áreas las atiendan y remitan las evidencias de su cumplimiento.

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

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, establece en su artículo 33 fracción VII, que el responsable deberá realizar, al menos, las actividades necesarias a efecto de 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.

Asimismo, los Lineamientos Generales de Protección de Datos Personales para el Sector Publico, en el artículo 63, fracción VII, señalan 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.

Motivo de lo anterior, la Unidad de Transparencia, en conjunto con la Coordinación de Repositorios, Investigación y Prospectiva, 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.

Por lo anterior, ante cualquier vulneración la Coordinación de Repositorios, Investigación y Prospectiva, deberá informar a la Unidad de Transparencia, lo antes posible cualquier evento respecto de alguna vulneración, informando lo siguiente:

- 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.

La Unidad de Transparencia registrará la alerta de seguridad y analizará en conjunto con la Coordinación de Repositorios, Investigación y Prospectiva, el impacto de la amenaza, así como la estrategia y medidas adoptadas, con la finalidad de evitar el incidente.

La Coordinación de Repositorios, Investigación y Prospectiva, deberá llevar una bitácora de las vulneraciones a la seguridad en la que se describa, la fecha en la que ocurrió, el motivo de ésta y las acciones correctivas implementadas de forma inmediata y definitiva.

III. MECANISMOS DE AUDITORÍA EN MATERIA DE DATOS PERSONALES

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

El establecimiento de las auditorias en materia de protección de datos personales, permitirá 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.

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.