• MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIAS DE SEGURIDAD

El artículo 30, fracción V, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Ley de Datos), estipula que, para cumplir con el principio de responsabilidad, es necesario implementar un sistema de supervisión y vigilancia que incluya auditorías para verificar que se están cumpliendo las políticas de protección de datos personales.

En línea con esto, el artículo 35, fracción VI, de la misma ley, establece que el documento de seguridad debe incluir, entre otras cosas, mecanismos para monitorear y revisar las medidas de seguridad implementadas.

Además, el artículo 33, fracción VII, de la Ley General establece que deben monitorearse y revisarse periódicamente los siguientes aspectos:

1. Las medidas de seguridad aplicadas para la protección de datos personales.
2. Las amenazas y vulneraciones a las que están expuestos los tratamientos o sistemas de datos personales.

Por su parte, el artículo 63 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales) establece que el responsable debe evaluar y medir los resultados de las políticas, planes, procesos y procedimientos en materia de seguridad y tratamiento de datos personales. Esto con el fin de verificar el cumplimiento de los objetivos establecidos y, en su caso, implementar mejoras continuas.

Para cumplir con esta obligación, el responsable debe realizar un monitoreo continuo de los siguientes aspectos:

Para cumplir con lo anterior, el responsable 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.

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 Instituto desarrollará el cumplimiento de dicha obligación a través de los siguientes mecanismos:

- Como un mecanismo de monitoreo, la Unidad de Transparencia rendirá informes semestrales al Comité de Transparencia en los que dé cuenta del avance de cumplimiento del Plan de Trabajo, así como de las novedades o cuestiones adicionales que estime conveniente hacer de su conocimiento.
- Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión;
- Revisión de cumplimiento de las políticas internas relacionadas con el tratamiento de datos personales a fin de asegurar que las personas servidoras públicas realicen los tratamientos de datos personales en concordancia con lo dispuesto en la Ley de Datos, los Lineamientos Generales, y demás normatividad que resulte aplicable.
- Revisará y, en su caso, actualizará los procesos involucrados en el tratamiento de datos personales.
- Revisar y, en su caso, actualizar los avisos de privacidad, las funciones y obligaciones del personal y los inventarios de datos personales.
- Revisión del riesgo. Tiene el objetivo de identificar modificaciones a los riesgos identificados en los tratamientos de datos personales,

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:

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

	Sí	No
1. Se han definido y 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 contempla medidas de seguridad específicas o adicionales a las previstas en la LGPDPPSO 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; • 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; • 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.	☐	☐
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: • 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.** 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

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 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.

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 la Gerencia de Servicios de Comunicaciones y Sistemas y de la Gerencia de Administración.

En el documento "Formato para registrar y reportar vulneraciones de datos personales" se concentran las actividades que deben realizare 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:
   - 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.

C. 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 de Datos, 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 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, con el siguiente fin:

- Verificar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados para el cumplimiento de las disposiciones previstas en la Ley de Datos Personales y los Lineamientos Generales.

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 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.

ELEMENTO A REVISAR	FUNDAMENTO	ACCIONES
Nuevos activos que se incluyan en la gestión de riesgos;	63, fracción I, de los Lineamientos Generales	Revisión del cumplimiento de la normatividad aplicable al tratamiento de los datos personales.
Modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras	63, fracción II, de los Lineamientos Generales	Revisión del cumplimiento de la normatividad aplicable al tratamiento de los datos personales.
Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas	63, fracción III, de los Lineamientos Generales	Revisión del cumplimiento de la normatividad aplicable al tratamiento de los datos personales Revisión del Riesgo: Monitoreo del entorno físico y electrónico
Posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes	63, fracción IV, de los Lineamientos Generales	Revisión del cumplimiento de la normatividad aplicable al tratamiento de los datos personales Revisión del Riesgo: Monitoreo del entorno físico y electrónico
Vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir	63, fracción V, de los Lineamientos Generales	Revisión del cumplimiento de la normatividad aplicable al tratamiento de los datos personales Revisión del Riesgo: Monitoreo del entorno físico y electrónico
Cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo	63, fracción VI, de los Lineamientos Generales	Revisión del cumplimiento de la normatividad aplicable al tratamiento de los datos personales Actualización del Plan de Trabajo y revisión de avances
incidentes y vulneraciones de seguridad ocurridas	63, fracción VII, de los Lineamientos Generales	Revisión del cumplimiento de la normatividad aplicable al tratamiento de los datos personales Vulneraciones a la seguridad de datos personales.