# Mecanismos de Monitoreo y Revisión de las Medidas de Seguridad

El artículo 33, fracción VII, de la Ley General establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, el monitoreo y revisión de manera periódica de las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales.

Como se señaló, de acuerdo con la fracción VI del artículo 35 de la Ley General, los mecanismos de monitoreo y revisión forman parte del documento de seguridad.

Así, respecto a los mecanismos de monitoreo y revisión de las medidas de seguridad, el artículo 63 de los Lineamientos Generales señala lo siguiente:

> ***Monitoreo y supervisión periódica de las medidas de seguridad implementadas***
> ***Artículo 63.*** *Con relación al artículo 33, fracción VII de la Ley General, 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 dispuesto en el párrafo anterior del presente artículo, el responsable deberá monitorear continuamente lo siguiente:*
>
> ***I.*** *Los nuevos activos que se incluyan en la gestión de riesgos;*
> ***II.*** *Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras;*
> ***III.*** *Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;*
> ***IV.*** *La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;*
> ***V.*** *Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;*
> ***VI.*** *El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y*
> ***VII.*** *Los incidentes y vulneraciones de seguridad ocurridas.*
>
> *Aunado a lo previsto en las fracciones anteriores del presente artículo, 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.*



De lo anterior es posible identificar que el monitoreo y revisión de las medidas de seguridad tiene el objetivo de fortalecer, a través de un ciclo de mejor continua, la protección de los datos personales que resguarda este Servicio de Protección Federal (SPF).

A continuación, se desarrollan las acciones de monitoreo y supervisión periódica para las medidas de seguridad del SPF:

## A. Mecanismos de monitoreo

Para los tratamientos de datos personales del SPF, se consideran los siguientes tipos de monitoreo:

1) **Revisión de cumplimiento de las políticas internas del SPF, relacionadas con el tratamiento de datos personales.** Tiene el objetivo de asegurar que los servidores públicos realicen los tratamientos de datos personales en concordancia con lo dispuesto en la Ley General, los Lineamientos Generales, y demás normatividad que resulte aplicable.

   Para ello, cuando se identifica algún cambio en los instrumentos antes mencionados, se deberán realizar las siguientes actividades:

   a. Revisar y, en su caso, actualizar los procesos involucrados en el tratamiento de datos personales.
   b. Revisar y, en su caso, actualizar los avisos de privacidad, las funciones y obligaciones del personal y los inventarios de datos personales, según corresponda.
   c. Evaluar si hubo cambios en las amenazas, vulnerabilidades o impacto de los riesgos relacionados con las modificaciones a la normativa, para actualizar los análisis de riesgos, análisis de brecha y plan de trabajo.
   d. Revisar y, en su caso, adecuar los sistemas de tratamiento para cumplir con los cambios normativos.

2) **Revisión del riesgo.** Tiene el objetivo de identificar modificaciones a los riesgos identificados en los tratamientos de datos personales, para ello, se implementarán los siguientes monitoreos:



   a. **Monitoreo del entorno físico.** Para la detección continua de amenazas y vulnerabilidades en el entorno físico, se cuenta con:
      I) Personal de vigilancia en los accesos al edificio del SPF,
      II) Control de acceso del personal con tarjeta de proximidad,
      III) Control de acceso a través de bitácoras para visitantes y personal del SPF que olvidó su credencial, y
      IV) Control de asistencia a través de huella digital.
   b. **Monitoreo del entorno electrónico.** Para la detección continua de amenazas y vulnerabilidades, la DTIC cuenta con herramientas automatizadas de monitoreo (activo y pasivo), así como con bitácoras de los sistemas informáticos del SPF
   c. **Actualización del plan de trabajo.** Derivado del monitoreo del entorno físico o electrónico, se pueden realizar actualizaciones en el plan de trabajo en caso de que se identifiquen cambios en las amenazas, las vulnerabilidades o el impacto de los riesgos identificados. Estos cambios se pondrán a consideración del área que apoya en el análisis de riesgos, la DTIC y el Comité de Transparencia.
   d. **Revisión de avances del plan de trabajo.** A través de los mecanismos que determine el área que apoya en el análisis de riesgos, la DTIC y el Comité de Transparencia, se hará una revisión de los avances en el plan de trabajo, identificando las acciones, fechas compromiso y, en su caso, las causas por las cuales no se está cumpliendo el plan de trabajo, para hacer los ajustes correspondientes al mismo.
   e. **Actualización tecnológica.** Cuando se integren nuevos equipos de cómputo, servidores, aplicaciones o tenga lugar una migración tecnológica, se realizará una actualización del análisis de riesgo.
   f. **Vulneraciones a la seguridad de los datos personales.** En caso de identificar un incidente de seguridad que involucre datos personales, el área que apoya en el análisis de riesgos, la

DTIC y el Comité de Transparencia se coordinarán para decidir sobre las acciones pertinentes para mitigar dicho incidente.

A continuación, se describen los mecanismos de monitoreo y revisión de este SPF:

| Elementos a revisar | Fundamento | Acciones |
|---|---|---|
| Los nuevos activos que se incluyan en la gestión de riesgos; | 63, fracción I, de los Lineamientos Generales. | 1. Revisión de cumplimiento de las políticas internas del SPF, relacionadas con el tratamiento de datos personales. |
| Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras; | 63, fracción II, de los Lineamientos Generales. | 1. Revisión de cumplimiento de las políticas internas del SPF, relacionadas con el tratamiento de datos personales.<br><br>2. Actualización tecnológica. |
| 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. | 1. Revisión de cumplimiento de las políticas internas del SPF, relacionadas con el tratamiento de datos personales.<br><br>• Monitoreo del entorno físico.<br>• Monitoreo del entorno electrónico. |
| La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes; | 63, fracción IV, de los Lineamientos Generales. | 1. Revisión de cumplimiento de las políticas internas del SPF, relacionadas con el tratamiento de datos personales.<br><br>• Monitoreo del entorno físico.<br>• Monitoreo del entorno electrónico. |
| Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir; | 63, fracción V, de los Lineamientos Generales. | 1. Revisión de cumplimiento de las políticas internas del SPF, relacionadas con el tratamiento de datos personales.<br><br>• Monitoreo del entorno físico.<br>• Monitoreo del entorno electrónico. |
| El 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. | 1. Revisión de cumplimiento de las políticas internas del SPF, relacionadas con el tratamiento de datos personales.<br><br>• Actualización del plan de trabajo.<br>• Revisión de avances del plan de trabajo. |
| Los incidentes y vulneraciones de seguridad ocurridas. | 63, fracción VII, de los Lineamientos Generales. | 1. Revisión de cumplimiento de las políticas internas del SPF, relacionadas con el tratamiento de datos personales.<br><br>• Vulneraciones a la seguridad de los datos personales. |



## B. Mecanismos de supervisión o revisión

Además del monitoreo continuo de las medidas de seguridad, se requiere realizar una supervisión periódica de las medidas de seguridad, a través de auditorías, las cuales pueden ser internas (desarrolladas por el propio SPF) o externas (realizando una contratación o a través de un convenio con un tercero).

Hasta el momento no se han realizado auditorías específicas en materia de protección de datos personales a los tratamientos del SPF.

Así, respecto del programa de auditoría mencionado en el último párrafo del artículo 63 de los Lineamientos Generales, se tiene contemplada la realización de una auditoría en materia de protección de datos personales, al menos una vez cada dos años. Dicha auditoría se puede llevar a cabo por terceros según la disponibilidad presupuestal, o bien internamente por personal del SPF, conforme lo determine el Comité de Transparencia.

El programa de auditoría será aquél que determine el Comité de Transparencia en el Programa de Protección de Datos Personales del SPF.

Los resultados de las auditorías se considerarán para realizar adecuaciones al análisis de riesgos del SPF y, por lo tanto, al plan de trabajo.