MECANISMOS DE MONITOREO DE SEGURIDAD DEL SISTEMA DE SUPERVICIÓN Y VIGILANCIA DE LA COMISIÓN NACIONAL FORESTAL.

UNIDAD DE TRANSPARENCIA.

Enero 2024

INTRODUCCIÓN.

De conformidad con el artículo 30, fracción V, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en el que señala los mecanismos que deberán adoptar los responsables para cumplir con el principio de responsabilidad, entre los cuales 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 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, controlando de manera periódica las medidas de seguridad implementadas en la protección de datos personales; así como las amenazas y vulneraciones a que están sujetos los tratamientos o sistemas de datos personales.

De igual manera, el artículo 63 de los Lineamientos Generales de protección de datos personales para el sector público establece que el responsable deberá evaluar y medir los resultados de las políticas, 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 de acuerdo a 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 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.

Por lo anterior, la CONAFOR generó los siguientes mecanismos:

A) 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 precisar:

1. Si se han definido y se mantienen las medidas de seguridad administrativas, técnicas y físicas necesarias para la protección de los datos personales de acuerdo a lo siguiente:

Declaración de confidencialidad	Administrativa
Listado de personal que interviene en el tratamiento de datos	Administrativa
Clasificación de los archivos físicos	Administrativa
Clasificación de los archivos electrónicos	Administrativa
Depuración y borrado seguro del archivo físico	Administrativa
Depuración y borrado seguro del archivo electrónico	Administrativa
Responsable de seguridad	Administrativa
Transferencias	Administrativa
Cuidado de los bienes informáticos	Física
No instalar equipos ajenos	Física
Prevenir accesos no autorizados	Física
Traslado de equipos de cómputo	Física
Archivero con candado	Física
Zona de confidencialidad	Física
Cuidado de la contraseña personal	Técnica
Actualización de contraseñas	Técnica
No instalar softwares	Técnica
Contraseñas robustas	Técnica
Respaldo de información	Técnica

2. Si 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 de conformidad a las previstas en la Ley y los Lineamientos Generales.

3. Si se han definido las funciones, obligaciones y cadena de mando de cada servidor público que trata datos personales, por unidad administrativa.

4. Si se ha comunicado a cada servidor público sus funciones, obligaciones y cadena de mando con relación al tratamiento de datos personales que efectúa.

5. Si se ha elaborado el inventario de Tratamiento de datos personales.

6. Si se ha realizado el análisis de riesgo.

7. Si se ha realizado el análisis de brecha.

8. Si 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

B) 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 oficio en el que se plasmarán las recomendaciones o requerimientos que se consideren pertinentes en materia de seguridad, con la finalidad de que las áreas administrativas las atiendan y remitan las evidencias de su cumplimiento.

Para medir los resultados en las medidas de seguridad y tratamiento de los datos personales, se deberán monitorear las vulneraciones de seguridad ocurridas, cuando se presenta alguna de las situaciones antes descritas, será obligatorio analizar las causas por las cuales se presentó dicha vulneración y así poder efectuar las acciones preventivas y correctivas para evitar que la vulneración afecte a más titulares o se vuelvan a repetir. Además, si la vulneración tiene el

riesgo de repercutir significativamente en los derechos patrimoniales o morales de sus titulares, se deberá informar sobre ésta, sin demora alguna, a los titulares afectados.

El anterior aviso, previene a los titulares para que puedan tomar las medidas correspondientes en la defensa de sus derechos, por lo que será necesario que cada área de la Comisión Nacional Forestal cuente con su propio registro de vulneraciones.

C) Etapa de actuación ante vulneraciones a la seguridad de los datos personales.

Cualquier persona que conozca sobre alguna vulneración de datos personales dentro de los sistemas de la Comisión Nacional Forestal, deberá informar inmediatamente a la persona responsable de la seguridad de datos personales que haya sido designada en el área de su adscripción.

A su vez, la persona responsable deberá informar inmediatamente sobre la violación a la persona titular del área de su adscripción y entablar contacto con la Unidad de Transparencia, a través de su titular, para informar el hecho y que ésta disponga lo conducente para orientar y acompañar en las gestiones que deban documentarse, las cuales deberán realizarse con celeridad para garantizar la eficacia de las medidas adoptadas.

La Unidad de Transparencia junto con la persona responsable, coordinarán las acciones preventivas que se estimen convenientes al interior del área de su adscripción para asegurar el cese inmediato de la vulneración, registrando los siguientes datos:

- El nombre y la clave de identificación registradas en el Inventario de Tratamientos de Datos Personales.
- El tratamiento de datos personales que fueran afectados.
- La persona que tuvo conocimiento de la vulneración del tratamiento de los datos personales.
- La fecha, hora y lugar en que tuvo conocimiento del hecho.
- Tipo de vulneración, pérdida o destrucción; robo, extravío o copia; uso, acceso o tratamiento; daño, alteración o modificación.

- Fecha y hora que tuvo conocimiento la Unidad de Transparencia respecto a la vulneración.

Una vez que fuera registrada esta información, se deberán formular las acciones correctivas de corto plazo, entre la Unidad de transparencia y las áreas competentes para subsanar la vulneración y evitar posteriores incidentes, asimismo, en cualquier caso se deberá informar a los titulares y/o al organismo garante sobre una vulneración que ponga en riesgo sus derechos patrimoniales o morales.

D) Revisiones y Auditoría

Dado que el riesgo no es estadístico ni se puede determinar de manera exacta, se deberá realizar un estudio de lo siguiente: las amenazas, vulnerabilidades, probabilidad y consecuencias que pudieran cambiar abruptamente sin previo aviso.

Por lo anterior, se acuerda ejecutar una revisión de cada riesgo por separado, así como la suma de ellos, para conocer el impacto potencial acumulado de las amenazas, así como también se deberá realizar las siguientes actividades de manera anual:

- Revisar los nuevos activos que se incluyan en los alcances de la gestión de riesgo.
- Realizar las modificaciones necesarias a los activos, por ejemplo, cambio o migración tecnológica.
- Analizar las nuevas amenazas que podrían estar activas dentro y fuera de la organización y que no han sido valoradas.
- Considerar, la posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes.
- Plasmar las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelven a surgir.
- Revisar el cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo.

La CONAFOR de acuerdo a sus Políticas Internas de Gestión y Tratamiento de Datos Personales, podrá monitorear y revisar la eficacia y eficiencia del sistema y las medidas de seguridad, también se podrán consideran las auditorías a través de externos para procesos y circunstancias especiales.

Las auditorías se llevan a cabo en intervalos de tiempo planeados para determinar si el sistema de monitoreo y seguridad, está operando de acuerdo con la política de gestión de datos personales y con los procedimientos establecidos, y si ha sido implementado de acuerdo con los requerimientos tecnológicos.

Finalmente, se deberán establecer las acciones correctivas implementadas y/o planeadas por las áreas competentes, así como las áreas involucradas en su consecución.