# SISTEMAS DE SUPERVISIÓN Y VIGILANCIA IMPLEMENTADOS EN LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS

## Introducción

La Comisión Nacional de los Salarios Mínimos, tiene el deber de evaluar y medir el resultado de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de datos personales, de conformidad con 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 y de más normatividad aplicable.

Asimismo, deberá contar con un sistema de gestión de seguridad de datos personales que permita planificar, establecer, implementar, operar, monitorear, mantener, revisar y mejorar las medidas de seguridad de carácter administrativo, físico y técnico aplicadas a los datos personales.

Corresponderá a la Unidad de Transparencia, y al Departamento de Tecnologías de la Información y comunicaciones, en el ámbito de su respectiva atribución, llevar a cabo, de manera coordinada y en conjunto con las unidades administrativas de la Comisión Nacional de los Salarios Mínimos, el diseño, la implementación y la mejora continua del sistema de gestión de seguridad de datos personales, con base en las necesidades institucionales. La elaboración y actualización periódica del documento de seguridad previsto en el artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados estará a cargo, de manera coordinada, de la Unidad de Transparencia y con la participación de las unidades administrativas de la entidad. En dicho documento deberán mencionarse, además, las medidas de seguridad implementadas para la protección de los datos personales.

## Normatividad aplicable

En cumplimiento del artículo 30, fracción IV, artículo 33 fracción VII y 35 fracción VI de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y artículo 63 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, la Comisión Nacional de los Salarios Mínimos ha formulado el presente documento.

En el caso de este sujeto obligado, la supervisión y la vigilancia que se llevará a cabo dentro de la misma institución la cual se llevará en tres etapas: una etapa inicial, una etapa intermedia y una etapa final, las cuales se describen de la siguiente manera:

## Etapa inicial

Se realizará un registro y recopilación de los tratamientos de datos personales en todas las Unidades Administrativas, verificar cuál es la vigencia de los mismos y, en su caso, determinar la modificación, actualización o cancelación de los mismos.
El proceso de lo anteriormente dicho, será el siguiente:

1. Solicitar a las Unidades Administrativas que señalen cuántos y cuáles son los sistemas de tratamiento de datos personales que se llevan a cabo;
2. Verificar que cada sistema de tratamiento de datos personales cuente con su inventario y descripción del ciclo de vida.
3. Emitir, en su caso, las observaciones correspondientes para implementar, modificar, actualizar o cancelar el sistema que se trate.

## Etapa intermedia

El objetivo de esta etapa es dar a las Unidades Administrativas la oportunidad de atender las observaciones que, en su caso, se les hayan hecho de conocimiento y con ello se mantenga la seguridad de los datos personales.
El proceso de lo anteriormente dicho, será el siguiente:

1. Asesorar a las Unidad Administrativas a las que se les hayan hecho observaciones a su o sus sistemas de tratamiento de datos personales para que puedan dar cumplimiento a las mismas.
2. Se les otorgará el tiempo necesario para cumplir con dichas observaciones y posteriormente revisar su cumplimiento, siendo máximo 20 días hábiles.
3. En caso de que haya incumplimiento parcial o total de las observaciones realizadas a las Unidades Administrativas, se deberán emitir unas nuevas y, de ser necesario, se citará al titular del área responsable del sistema de tratamiento de datos personales a la sesión del Comité de Transparencia próxima a realizar, con la finalidad de que manifiesta las causas del incumplimiento y se otorgue tiempo para su cumplimiento.

Agregando a esta etapa intermedia, en caso de que se presente una vulneración a la seguridad de los datos personales en posesión de esta entidad, el titular de la unidad administrativa involucrada, deberá dar aviso a la Unidad de Transparencia, remitiendo un informe en el que se indique cuando menos lo siguiente:

a) La naturaleza del incidente, particularmente si se considera que afecta de forma significativa los derechos patrimoniales o morales del titular cuando la vulneración esté relacionada, de manera enunciativa mas no limitativa, con sus bienes muebles e inmuebles. Por otro lado, se entenderá que se afectan los derechos morales del titular cuando la vulneración esté relacionada, de manera enunciativa mas no limitativa, con sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, configuración y aspecto físico.
b) Las circunstancias de modo, tiempo y lugar en la que la vulneración haya ocurrido.
c) Las categorías y número aproximado de titulares afectados.
d) Los sistemas de tratamiento y datos personales comprometidos.
e) La descripción de las posibles consecuencias en la vulneración de la seguridad ocurrida.

f) Una propuesta sobre las medidas de los titulares de los datos comprometidos, en su caso, podrían adoptar para proteger sus intereses.
g) Las acciones correctivas que haya llevado a cabo, y las que en su caso sugiera implementar.
h) Las recomendaciones dirigidas al titular.
i) Los medios a través de los cuales los titulares, en su caso, podrían obtener más información al respecto.

De manera enunciativa mas no limitativa, se entenderá por vulneración de seguridad:

- La pérdida o destrucción no autorizada;
- El robo, extravío o copia no autorizada;
- El uso, acceso, tratamiento no autorizado, o
- El daño, la alteración o modificación no autorizada.

Una vez que la Unidad de Transparencia reciba la noticia de alguna vulneración a datos personales se convocará a sesión extraordinaria con el fin de que se tomen las determinaciones correspondientes en el ámbito de sus atribuciones y se coordine la instrumentación de acciones previstas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales de Protección de Datos Personales en el Sector Público.

Cabe aclarar, que el Departamento de Tecnologías de la Información y Comunicaciones, dentro de la Comisión Nacional de los Salarios Mínimos, ha implementado medidas de seguridad entre las que destacan:

- El envío de correos electrónicos para concientizar a la gente para que realicen respaldos de seguridad de los discos asignados o en las carpetas de RED del servidor de repositorios;
- Creación de carpetas compartidas para la Dirección de Administración y Finanzas y sus diversas áreas para respaldar información delicada y/o vulnerable;
- Realización de cambios a contraseñas de los servidores de manera constante;

- Instalación de un aparato biométrico con administración del mismo para el acceso del SITE de la entidad;
- Instalación de una cámara IP en el SITE para el monitoreo de acceso al mismo.

Aunado a lo anterior, dicho Departamento de Tecnologías continua con la labor de actualización de las medidas de seguridad con el objetivo de que exista un mayor respaldo en caso del surgimiento de amenazas.

## Etapa final

Esta última etapa se divide en dos puntos; el primero de ellos es si a la unidad administrativa responsable no le fueron emitidas observaciones a resolver o, en su caso, fueron emitidas, pero resueltas de manera satisfactoria; el segundo punto es acerca del proceso que se seguirá para solventar las vulneraciones a la seguridad de los datos personales en posesión de la Comisión Nacional de los Salarios Mínimos;

1. En el caso en que no se hayan emitido observaciones, o bien, habiéndose emitido éstas, se cumplieron satisfactoriamente, se desarrollarán las siguientes actividades:
    a. Someter a aprobación del Comité de Transparencia la implementación, modificación, actualización o cancelación de los sistemas de tratamiento de datos personales.
    b. Hacer de conocimiento del Comité de Transparencia la versión final del documento de seguridad.
    c. Hacer la difusión correspondiente del documento de seguridad entre las unidades administrativas.
2. Se deberá llevar a cabo el monitoreo de la seguridad de los datos personales, con base en los mecanismos que las unidades administrativas tengan implementadas para esos efectos, así como la información que deba proporcionarse. Dicho monitoreo tendrá como propósito conocer de manera periódica el estado de control, con la finalidad de obtener seguridad de las acciones de mejora continua que se llevan a cabo. El resultado de las actividades de monitoreo y verificación, deberán ser informadas ante el

Comité de Transparencia a efecto de que se esté en posibilidad de actuar en el ámbito de sus atribuciones.

3. Las medidas de seguridad con las que la Comisión Nacional de los Salarios Mínimos cuenta para evitar vulneraciones es que se cuenta con un servidor de repositorios para realizar respaldos cada mes de los servidores de la entidad y de la información de las áreas que lo soliciten; asimismo, se deja copia de seguridad anterior para tener más seguridad en la reparación de este. Otra de las medias con las que se cuenta es una pared de fuego Fortinet para eliminar las amenazas entrantes, así como un software antivirus.

Asimismo, la Comisión Nacional de los Salarios Mínimos continua con el monitoreo continuo de:

1. Los nuevos activos que se incluyan en la gestión de riesgos (activo es todo elemento de valor involucrado en el tratamiento de datos personales, como pueden ser una base de datos, el conocimiento de los procesos, el personal, el hardware, el software, los archivos o los documentos en papel).
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.