DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES DE LA COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS

TRABAJO
SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL
CONASAMI
COMISIÓN NACIONAL DE LOS SALARIOS MÍNIMOS

Índice

1. Presentación.

La Constitución Política de los Estados Unidos Mexicanos en los artículos 6 y 16 incorpora el derecho de toda persona a la protección de sus datos personales, así como al acceso, rectificación, cancelación y oposición en los términos que determina la ley.

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO o Ley General) establece por su parte un conjunto de bases, principios y procedimientos para garantizar el derecho a la protección de datos con carácter personal y que se encuentren en posesión de los sujetos obligados, entre los que figura la Comisión Nacional de los Salarios Mínimos (CONASAMI) como órgano técnico del Poder Legislativo.

De ahí que el presente **Documento de Seguridad** tiene como propósito establecer el marco de referencia del tratamiento de los datos personales que se llevan a cabo al interior de la CONASAMI por las diversas unidades administrativas que conforman su estructura orgánica, para mantener vigente y promover la mejora continua en la protección de los mismos, en términos de lo previsto en los artículos 35 y 36 de la LGPDPPSO, además de desarrollar buenas prácticas en la materia.

En ese sentido, la CONASAMI ha identificado los procesos que en el ámbito de su competencia involucran el tratamiento de datos personales, a efecto de mantener la seguridad de losmismos durante el ciclo de vida de la información, indicando la forma en la que se trata,las medidas de seguridad adoptadas y las áreas responsables de su protección, así como las finalidades del tratamiento de acuerdo a sus respectivos ámbitos de funciones.

Considerando que los datos personales constituyen el principal activo de información objeto del presente documento, es necesario señalar que todos y cada uno de los elementos que lo integran, constituyen un sistema interno para la gestión y tratamiento de los datos personales en posesión de la CONASAMI, pues tal y como lo dispone el artículo 34 de la LGPDPPSO, se entiende por sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, operar, monitorear, mantener y mejorar el tratamiento y seguridad de los datos personales.

Así, la CONASAMI comprometida con la tutela de los datos personales que trata y, acorde a larecomendación emitida por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, ha impulsado a su interior las acciones conducentes para evitar la alteración, pérdida, transmisión y acceso no autorizados a los datos, mediante la implementación de medidas físicas, administrativas y técnicas, tendentes a garantizar la seguridad e integralidad de los mismos, así como su seguimiento y supervisión continuos.

De ahí, que dicho Sistema permita disponer de información relacionada con las medidas de seguridad, el análisis general de las amenazas y posibles vulnerabilidades, así como los mecanismos o acciones a implementar para mitigarlas.

Dicho lo anterior, el presente documento se integra a partir la gestión de actividades coordinadas para controlar y verificar que el tratamiento de los datos personales sea acorde con los principios que rigen su protección, pues para la CONASAMI la política de seguridad en esta materia constituye un compromiso con el cumplimiento de las disposiciones previstas tanto en la citada LGPDPPSO, como en los Lineamientos Generales de Protección de Datos Personales para el Sector Público por parte de todos los involucrados.

Para ello, en términos de lo previsto en el artículo 36, fracción II de la Ley General, el cual establece que los responsables deberán mantener actualizado su documento de seguridad como resultado del proceso de mejora continua, la CONASAMI a partir de la aprobación del *Acuerdo por el que se reforman, adicionan y derogan diversas disposiciones del Reglamento Interior*, llevó a cabo un proceso de rediseño institucional en el que se crean nuevas unidades administrativas y establecimiento de nuevas funciones y atribuciones, acorde con los fines de la propia Institución, lo cual, ha propiciado la actualización de diversos elementos, tales como los **inventarios de datos personales**; las **medidas de seguridad** adoptadas con motivo de su tratamiento y, el **análisis de riesgo y brecha**, con el objeto de monitorear las medidas adoptadas, identificar posibles vulneraciones y mitigar los riesgos; además de avanzar en un proceso de sensibilización permanente respecto de la relevancia que tiene para la institución adoptar medidas correctivas y preventivas, en función de los resultados obtenidos de la revisión de los sistemas de datos, a la luz los esquemas de autorregulación y capacitación del personal.

2. Objetivo y alcance del documento.

Establecer los principales elementos que integran las medidas de seguridad administrativas, físicas y técnicas que ha adoptado la CONASAMI para garantizar la confidencialidad, integridad y disponibilidad de los datos personales; así como determinar las posibles vulnerabilidades, amenazas y riesgos de los que pueden ser objeto en un plano general los diverso sistemas de información y procesos en los se tratan datos personales por las diversas unidades administrativas, conforme a lo establecido en la LGPDPPSO y a los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

En este sentido, la Dirección General de Transparencia integra el presente documento de seguridad con base en la información generada por las citadas unidades administrativas acorde al ámbito de sus funciones y, de conformidad con las disposiciones aplicables.

3. Sistema de gestión de los datos personales en posesión de la CONASAMI.

Para el tratamiento de los datos personales que lleva a cabo la CONASAMI a través de su obtención, uso, registro, conservación, acceso, manejo, aprovechamiento, transferencia, disposición o cualquier otra operación aplicable a los mismo, se realiza el establecimiento de políticas y métodos orientados a salvaguardar su confidencialidad, integridad y disponibilidad, conforme a los preceptos previstos por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y la Ley General de Transparencia y Acceso a la Información Pública.

En tal virtud, la CONASAMI inició su proceso de planificación de los esquemas de protección de datos mediante la identificación de todos y cada uno de los procesos y tareas en los que, de acuerdo con el ámbito de funciones de las distintas áreas que conforman la institución, se involucra el tratamiento de datos personales. Para ello, se dispuso de un formato que permitió a las diversas unidades administrativas realizar el levantamiento de inventarios de los datos personales que se encuentran bajo su responsabilidad, considerando los elementos mínimos que establece el artículo 33, fracción II de la Ley General y el diverso 58 de los Lineamientos Generales de Protección de DatosPersonales para el Sector Público.

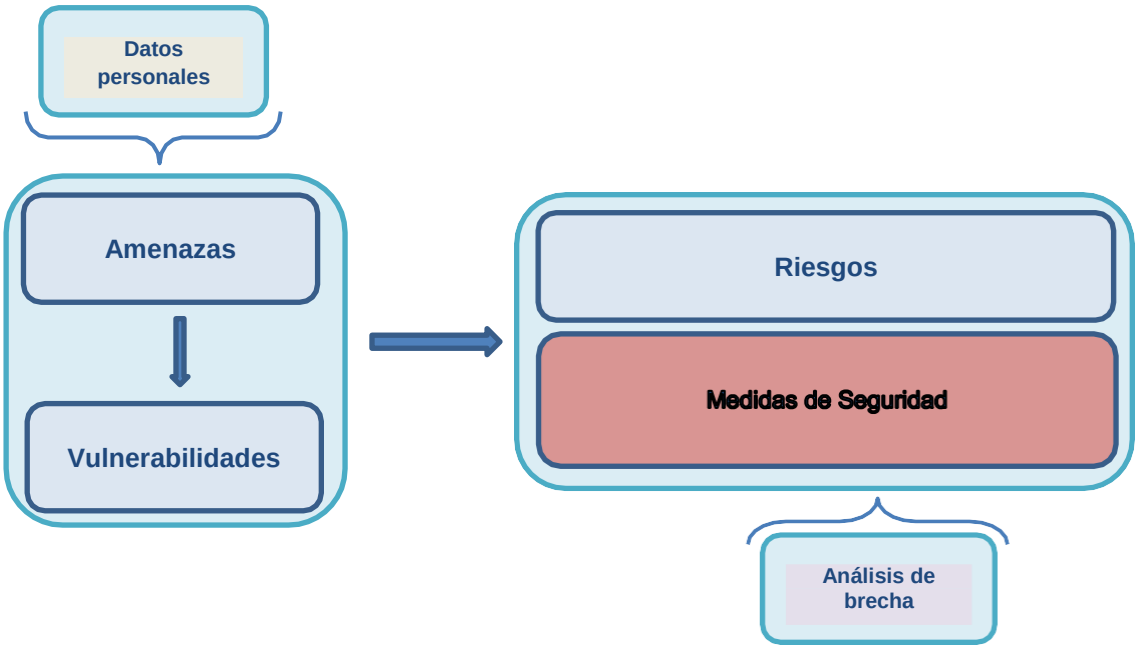
Es así que a través del desarrollo de un instrumento homogéneo y estandarizado, se llevó a cabo el levantamiento del **inventario de datos,** con el propósito de identificar, entre otros aspectos, la categoría y tipo datos que son sometidos a tratamiento, incluyendo los de carácter sensible; los medios a través de los cuales se obtienen dichos datos; el sistema físico y/o electrónico que se utiliza para su acceso, manejo, aprovechamiento, monitoreo y procesamiento; las características del lugar donde se ubican las bases físicas o electrónicas de datos; las finalidades del tratamiento, y el nombre, cargo y adscripción de los servidores públicos que tienen acceso al tratamiento, además de si son objeto de la transferencia y la identificación de los destinatarios o receptores de los mismos, así como las causas que la justifican.

En ese mismo sentido, el inventario ha contribuido desde el punto operativo a considerar el ciclo de vida de los datos personales, de forma tal que los servidores públicos que intervienen en el tratamiento conocen que, una vez concluida la finalidad los datos, éstos deben ser sometidos a un proceso de bloqueo y, en su caso, de cancelación, supresión o destrucción, lo que cobra especial relevancia en el marco del proceso de baja documental que las áreas realizan conforme a las disposiciones que regulan la gestión documental al interior de la Institución.

De igual forma, una vez integrados los inventarios de datos, se dispuso de la metodología para la elaboración del análisis de riesgos, en la cual, atendiendo a lo previsto en el artículo 33, fracción IV de la Ley General de la materia, las áreas responsables de su tratamiento identificaron el valor de los datos personales de acuerdo con su categoría y el ciclo de vida; el valor de exposición de los activos involucrados en el tratamiento; las consecuencias que pueden generarse para los

titulares de los mismos con motivo de su posible vulneración y, los factores de riesgo a los que eventualmente se encuentran expuestos.

Con base en dicho análisis de riesgo, además de promover el reconocimiento de las medidas de seguridad ***administrativas,*** entendidas como el conjunto de políticas y procedimientos de gestión, soporte y revisión de la seguridad de la información; ***físicas***, que corresponden a las acciones o mecanismos para proteger el entorno físico de los datos, así como de los recursos involucrados en su tratamiento y, ***técnicas*** que se valen de la tecnología para proteger el entorno digital de la información, también se han registrado nuevas medidas de seguridad que deberán desarrollarse para fortalecer algunos de los controles que actualmente son implementados; es decir, el análisis de brecha a partir del cual será posible mitigar los riesgos a los que están expuestos los datos tratados, tal y como se ilustra a continuación el siguiente esquema[1]:



Considerando que la identificación de **vulnerabilidades** tiene por objeto prevenir posibles dificultades en la seguridad de los datos bajo un enfoque proactivo; es decir, identificar áreas de oportunidad en materia de seguridad de datos personales sin que éstas constituyan un daño efectivo, es que se listan como posibles vulnerabilidades, las siguientes:

1. Controles de acceso físico y electrónicos inadecuados a sistemas de archivos.

2. Deficiente conocimiento de procedimientos en materia de seguridad de datos.

3. Inadecuada administración de autorizaciones de accesos a los datos personales (sistemas de privilegio).

[1] Integrado con base en el ciclo PHVA, establecido en las Recomendaciones en materia de Seguridad de Datos Personales, publicado por el entonces IFAI, en el DOF el 30 de octubre de 2013, consultable en http://dof.gob.mx/nota_detalle.php?codigo=5320179&fecha=30%2F10%2F2013

4. Falta de definición de perfiles y roles para delimitar funciones manejo y uso de datos.
5. Falta de seguimiento y monitoreo a políticas de seguridad.

6. Ausencia de mecanismos de confidencialidad por parte del personal (interno) o por terceros (externos).

Aunado a las anteriores vulnerabilidades, de manera enunciativa más no limitativa, se examinan algunos tipos de amenazas, que pueden ser intencionales o no, a las que podría enfrentarse la institución y sus activos de información.

TIPOS DE AMENAZAS
• Robo, extravío o copia no autorizada. • Uso, acceso o tratamiento no autorizado. • Daño, alteración o modificación no autorizado. • Pérdida o destrucción no autorizada. • Otras.

El riesgo que de manera general puede presentarse en caso de que las amenazas señaladas exploten las vulnerabilidades, es el de facilitar el acceso a los datos personales de manera no autorizada con el fin de comprometer su confidencialidad, disponibilidad e integridad, por lo que las medidas de seguridad por parte de las áreas comisionadas están orientadas a proteger los datos personales.

A partir de la identificación de vulnerabilidades y amenazas, se han establecido medidas de seguridad generales, que de acuerdo a la experiencia y mejores prácticas son monitoreadas para lograr la mejora continua por parte de todos los involucrados en el tratamiento. Como parte del sistema de gestión y política de seguridad institucional, se enmarcan las reglas generales siguientes:

a) Tratar datos personales de manera lícita, conforme a las disposiciones establecidas por la Ley General;

b) Sujetar el tratamiento de los datos personales al principio de consentimiento, salvo las excepciones previstas por la Ley;

c) Informar a los titulares del tratamiento de los datos y sus finalidades;

d) Procurar que los datos personales tratados sean correctos y estén actualizados;
e) Suprimir los datos personales cuando hayan dejado de ser necesarios para las finalidades para las cuales se obtuvieron;

f) Tratar los datos personales estrictamente para propósitos legales o legítimos de la CONASAMI;

g) Limitar el tratamiento de los datos personales al cumplimiento de las finalidades;

h) No obtener datos personales a través de medios fraudulentos;

i) Respetar la expectativa razonable de privacidad del titular;

j) Tratar estrictamente los datos personales necesarios, adecuados y relevantes en relación con las finalidades;

k) Velar por el cumplimiento de los principios;

l) Establecer y mantener medidas de seguridad;

m) Guardar la confidencialidad de los datos personales;

n) Identificar el flujo y ciclo de vida de los datos personales;

o) Mantener actualizado el inventario de datos personales o de las categorías que maneja la CONASAMI;

p) Respetar los derechos de los titulares en relación con su datos personales;

q) Aplicar las excepciones contempladas en la normativa en materia de protección de datos personales, y;

r) Identificar a los servidores públicos de la CONASAMI responsables del tratamiento de losdatos personales.

Con base en lo anterior, la CONASAMI determina las pautas de acción del personal encargado de tratamiento de datos personales con miras a generar su correcto resguardo, buscando en todo momento actuar en apego a las directrices de la LGPDPPSO y los Lineamientos de la materia, siempre en consideración de la salvaguarda del derecho ala privacidad y protección de datos de las personas.

4. Análisis de riesgos y de brecha.

El presente análisis identifica el riesgo inherente a los datos personales en el tratamiento que reciben por la Comisión Nacional de los Salarios Mínimos (CONASAMI) al ejercer sus atribuciones, de manera que pueda ser controlado por la institución para satisfacer el derecho humano a la autodeterminación informativa.

La LGPDPPSO en sus artículos 32, fracción I, y 33, fracción IV, considera que el determinar el riesgo inherente a los datos personales tratados es un deber de los sujetos obligados en la adopción de medidas de seguridad, para lo que deben realizar un análisis que considere las amenazas y vulnerabilidades para los datos, así como los recursos involucrados en el tratamiento.

Con base en la LGPDPPSO, la valoración de los riesgos de los datos personales forma parte de los elementos mínimos que debe contener el instrumento que describe y da cuenta, en lo general, sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas (Documento de seguridad), en este caso, por la CONASAMI, con el propósito de garantizar la confidencialidad, integridad y disponibilidad de ese tipo de datos bajo su posesión.

Aunado a lo anterior, los Lineamientos Generales de Protección de Datos Personales para el Sector Público, emitidos por Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), indican en su artículo 60 que el análisis de riesgos de los datos personales tratados debe contemplar los siguientes aspectos:

- 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 de los datos personales, que puedan derivar en una vulneración de seguridad.
- El riesgo inherente, la sensibilidad, las posibles consecuencias de vulneración para los titulares, las transferencias y vulneraciones previas ocurridas sobre los datos personales, así como el número de titulares de éstos y el riesgo por su valor potencial, además del desarrollo tecnológico.

Elementos para el análisis de riesgos

La seguridad de los datos personales que se tratan en la CONASAMI demanda conocer y entender los riesgos a los que se encuentran expuestos en los distintos procesos que realizan las unidades administrativas, lo que permitiría afrontarlos de manera adecuaday oportuna.

Para analizar los riegos de los datos personales que son objeto de tratamiento por la CONASAMI, se elaboró un instrumento que, a partir de considerar su objeto y atribuciones constitucionales, clasifica los datos en tres tipos, tal y como ha sido referenciado con antelación.

1) De **identificación o contacto**, que se refieren a información por la que se identifica a una persona y/o permiten su contacto como, por ejemplo, el nombre, el domicilio, el correo electrónico, la firma, los usuarios, el Registro Federal de Contribuyentes, la Clave Única de Registro de Población o la edad.

2) **Patrimoniales**, que comprenden la información que se encuentran vinculados al patrimonio de una persona como, por ejemplo, el salario, los créditos, las tarjetas de débito, los cheques o las inversiones.

3) **Sensibles**, que consideran la información concerniente a la esfera más íntima de su titular o que su uso puede dar origen a discriminación o conlleva un riesgo grave para éste como, por ejemplo, el origen étnico, el estado de salud presente o futuro, las creencias religiosas, la opinión política o la orientación sexual.

Para la determinación del riesgo sobre esa tipología de datos personales se valora la probabilidad e impacto de que, en su obtención, almacenamiento, tratamiento, transferencia o remisión, bloqueo y/o eliminación (ciclo de vida), en correspondencia con una diversidad de activos involucrados, se materialice uno o más factores que pueden causar un daño a su titular (amenaza). Para facilitar el análisis, se establecieron cuatro tipos de amenazas:

- Robo, extravío o copia no autorizada.
- Uso, acceso o tratamiento no autorizado.
- Daño, alteración o modificación no autorizado.
- Pérdida o destrucción no autorizada.
- Otras*

Esto es, se tomó en cuenta la probabilidad baja, media o alta de que la amenaza suceda en las distintas etapas de vida de los datos personales. Así, se consideró la consecuencia desfavorable leve, moderada o grave que al titular provoca en caso de que la amenaza ocurra (impacto).

La identificación y valoración del riesgo en cada proceso en que se tratan datos personales por las unidades administrativas de la CONASAMI se basaron en una escala del 0al 3, representándose de la forma siguiente:

Rango	**Valor del Riesgo**
Cuando el valor es < = 1	Bajo
Cuando > 1 y < 2	Medio
Cuando el valor es > = 2	Alto

* En la identificación de los riesgos al interior de la CONASAMI, la categoría de amenaza “Otras” se actualizo únicamente en la etapa de almacenamiento, la cual se enuncio como “Fenómenos sísmicos, fuego y pérdida de suministro eléctrico”.

5. Medidas de seguridad generales.

Las medidas generales de seguridad administrativas, físicas y técnicas con las que actualmente cuenta la CONASAMI para mantener la confidencialidad e integralidad de la información, así como para proteger los datos personales contra daño, pérdida, destrucción o alteración, así como evitar el uso, acceso o tratamiento no autorizado, e impedir la divulgación no autorizada, son las siguientes:

a) Medidas administrativas.

1. Adopción de un esquema de capacitación permanente en materia de la Ley General de Protección de Datos Personales en posesión de Sujetos Obligados (LGPDPPSO), impartido mediante el Campus Virtual de Capacitación del organismo garante.

2. Implementación de formatos de entrada y salida de préstamo de documentos por parte del área encargada del archivo.

3. Resguardo de los expedientes bajo los criterios, directrices y lineamientos para la atención de los expedientes técnicos.

4. Mecanismos de control desarrollados conforme a lo establecido en los lineamientos del Sistema de Gestión de Documentos institucional.

5. Suscripción de una carta responsiva por parte de los usuarios o personal con acceso a sistemas de datos personales, acerca del deber de confidencialidad.

6. Reportar al superior jerárquico los incidentes detectados respecto de pérdida o alteración de cualquier documento que contengan datos personales.

b) Medidas físicas.

1. Resguardo de documentos e información en archivos físicos de trámite y concentración.

2. Disponer de la instalación de chapas con llave para mantener control de acceso de personas a espacios de resguardo de información.

3. Limitar el número de personas con acceso a archivos físicos.

4. Realizar el registro de personas con acceso a espacios físicos en los que se resguarda información con datos personales.

5. Procurar suscribir responsivas de confidencialidad con el personal que trata datos personales.

6. Designación de personal con acceso controlado a espacios de resguardo físico de expedientes y documentos con datos personales.

7. Resguardo de llaves en oficinas de acceso restringido.

c) Medidas técnicas.

1. Utilizar claves de usuario y contraseñas de manera personal, y evitar compartirlas, prestarlas o registradas a la vista de otras personas.

2. Establecer y utilizar contraseñas robustas, es decir, de al menos ocho caracteres alfanuméricos y especiales, evitando que sean iguales al nombre del usuario, o cualquier otro nombre de personas, considerando que éstas sean fáciles de recordar y difíciles de adivinar o descifrar por un tercero, a fin de salvaguardar la información y datos personales a los que se tenga acceso.

3. Notificar de manera inmediata a la Dirección General de Sistemas los casos en los que los usuarios identifiquen o consideren que sus claves de usuario y/o contraseñas han sido utilizadas por un tercero.

4. Utilizar el correo electrónico para fines relacionados con las actividades laborales, evitando remitir datos personales.

5. Mantener los documentos electrónicos y físicos en lugares seguros, bajo llave, dentro de cajones cerrados, o bajo la protección de alguna contraseña, a fin de promover la restricción a los datos personales que pudieran contener.

6. No difundir, transmitir o compartir documentos electrónicos ni físicos que contengan datos personales, a fin de garantizar que estos no sean divulgados de manera no autorizada.

7. Evitar dejar u olvidar los documentos físicos que contengan datos personales en los equipos de impresión, así como evitar su impresión, escaneo y fotocopiado si no es realmente requerido para las actividades laborales.

8. Evitar el acceso a los sistemas de información de tratamiento de datos personales, bajo el precepto del mínimo privilegio; es decir, únicamente al personal que por sus funciones y facultades laborales los requiera, a fin de mantener una adecuada segregación de funciones, restricción de acceso y tratamiento de esos datos.

9. Borrar o eliminar de la papelera de reciclaje del escritorio de los equipos de cómputo los documentos o archivos electrónicos que nos son necesarios para el desarrollo de funciones.

10. Notificar las bajas de accesos a los sistemas de información o de tratamiento de datos personales, con oportunidad, para restringir el acceso a dichos datos por personal no autorizado.

Adicionalmente, como parte de la política de seguridad técnica, la Dirección General de Sistemas implementa los siguientes controles:

1. Definición de políticas de contraseñas.
2. Asignación privilegios de acuerdo a roles y funciones.
3. Agente de seguridad instalado en administrativos de servidores de correo electrónico.
4. Tareas de respaldo por servidor y por agente.
5. Autenticación de correo electrónico.
6. Operación *Hardening* en los servidores de Información en alta disponibilidad con contraseña de directorio de datos y acceso restringido.
7. Tareas de respaldo por servidor y de las instancias de base de datos del servicio.
8. Acceso a los sistemas conforme a procedimiento de administración de usuarios y contraseñas con cuenta local con permiso de administrador.
9. Borrado seguro de la información que reside en los equipos de cómputo.
10. Deshabilitación de cuentas de personal que causa baja.
11. Acceso controlado de administración y accesos privilegiados.
12. Definición de procedimientos y controles de seguridad de la información.

6.1 Monitoreo de las medidas de seguridad.

La supervisión de las medidas de seguridad técnicas y físicas es un elemento importante para la mejora continua, pues permite definir nuevos controles de monitoreo y seguimiento de éstas. Entre las medidas de supervisión y monitoreo se encuentran las siguientes:

1. Revisar la actualización permanente del esquema de contraseñas conforme a las pantallas de parametrización de los sistemas, verificando que los valores se encuentren determinados conforme a la política.
2. Monitorear que todas las cuentas que se dan de alta para otorgar acceso a la red, sea validada en el campo correspondiente a la contraseña, a fin de asegurar el uso.
3. Revisar el cumplimiento de protocolos.

4. Validar que los accesos, baja o cambio a sistemas se realicen conforme al proceso de administración de usuarios.

5. Vigilar que el ingreso de personas sea a través de los accesos correspondientes, plenamente identificados.

7. Propuesta de capacitación en materia de datos personales.

Uno de los factores esenciales para la implementación de los controles y demás medidas de seguridad, la actualización y mejora continua del inventario de datos personales, el apego a la normatividad y a Ley, así como la concientización en la materia por parte del personal involucrado en el tratamiento de datos personales, es el conocimiento y capacitación, por lo que el aprovechamiento de los recursos y herramientas que el propio Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) ha dispuesto para su uso y obtención de beneficios, se propone que a través del Instituto de Capacitación y Desarrollo en Fiscalización Superior, en coordinación con la Dirección de Colaboración Institucional y Vinculación con el Sistema Nacional de Transparencia, se desarrolle un programa de capacitación focalizada, mediante el cual profundice en el conocimiento de la materia por parte de los servidores públicos que intervienen en el tratamiento de datos personales.

Así, entre los elementos de los que resulta necesario profundizar se encuentran los siguientes:

I) Introducción al derecho a la protección de datos personales.

- ✓ Principios.
- ✓ Deberes.
- ✓ Sistemas de datos personales.
- ✓ Medidas de seguridad.
- ✓ Procedimientos y sanciones/ Derechos ARCO (acceso, rectificación, cancelación y oposición).
- ✓ Medios de defensa.

II) La LGPDPPSO y sus Lineamientos.

- ✓ Antecedentes.
- ✓ ¿A quién aplica?
- ✓ ¿Qué objeto tiene?

III) Fundamentos conceptuales de la LGPDPSO.

- ✓ Inventario y Base de Datos.

- ✓ Medidas de seguridad.
- ✓ Análisis de brecha y de riesgo.
- ✓ Funciones y obligaciones.

IV) Relevancia de los Avisos de Privacidad.

- ✓ Consentimiento.
- ✓ Deber de información.
- ✓ Finalidades del tratamiento de los datos.

8. Funciones y responsabilidades del tratamiento de datos personales.

A raíz de los procesos determinados en el Inventario de Datos Personales, por las áreas que integran las unidades administrativas que realizan tratamiento de éstos dentro de la Comisión Nacional de los Salarios Mínimos, resultó necesario asociar dichas actividades con las facultades que el Reglamento Interior otorga a los servidores públicos responsables de dicho tratamiento, a efecto de generar certeza y dar cumplimiento al principio de legalidad que debe atender todo servidor público.

9. Programa de trabajo para la implementación de medidas de seguridad.

Conforme al análisis de brecha, existen algunas medidas de seguridad que se requiere implementar, por lo que a continuación se presentan las actividades generales que se planea realizar:

- Celebración de reuniones de trabajo con unidades administrativas a efecto identificar alternativas de solución técnicas, físicas y administrativas a desarrollar en el mediano y largo plazo.

- Promover un sistema de gestión y administración de datos personales que permita centralizar mediante la identificación de datos por categorías, asociando los diversos tratamientos y procesos a las políticas de seguridad que resultan aplicables a cada caso, conforme a los estándares y mejores prácticas en la materia.

- Implementar mecanismos de divulgación y conocimiento de las políticas generales de seguridad y, verificar de manera continua su cumplimiento.

- Fortalecer los mecanismos de control de documentos e información en las distintas unidades administrativas, a efecto de evitar posibles vulneraciones.