Programa de mejora continua del Sistema de gestión de seguridad y protección de datos personales (SGSPDP) para el Centro Nacional de Metrología.

Introducción.

En virtud de la implementación del Sistema de gestión de seguridad protección de datos personales (SGSPDP), El Centro Nacional de Metrología (CENAM) tiene el deber de evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, de conformidad con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales) y demás normatividad aplicable.

En ese sentido, existe la obligación y la necesidad de generar un Programa de mejora continua específico para el CENAM, con la finalidad de verificar el cumplimiento de los objetivos propuestos y, en su caso, implementar mejoras de manera continua.

Propósito del Programa

Que el SGSPDP se mantenga vigente y actualizado, realizando las modificaciones necesarias que permitan mantener de manera efectiva la protección en el tratamiento de los datos personales que llevan a cabo los servidores públicos en el ejercicio de sus atribuciones.

En cumplimiento del artículo 30 fracción IV, artículo 33 fracción VII y 35 fracciónVI de la LGPDPPSO y artículo 63 de los Lineamientos Generales, el CENAM, ha formulado el presente Programa de mejora continua en la materia, con una visión práctica para implementar los nuevos tratamientos de datos personales, modificar o actualizar los existentes y cancelar aquellos que ya no estén vigentes.

Para la operación del Programa, cada año se elaborará un Cronograma de trabajo que incluya las siguientes etapas y actividades:

Etapa inicial

Una de las primeras acciones a realizar en esta etapa, es la de realizar un censo de los tratamientos de datos personales en todas las Unidades Administrativas, a través de los enlaces de datos personales que sean designados, a efecto de verificar que estén integrados al SGSPDP, cuál es su vigencia y determinar, en su caso, la modificación, actualización o su cancelación.

En virtud de lo anterior, en esta etapa se desarrollarán las siguientes actividades:

1) Solicitar a las Unidades Administrativas que señalen cuántos y cuáles son los sistemas de tratamiento de datos personales que llevan a cabo.

2) Verificar que cada sistema de tratamiento de datos personales cuente con su inventario, descripción del ciclo de vida y sus avisos de privacidad (simplificado e integral).

3) Emitir, en su caso, las observaciones correspondientes para implementar, modificar, actualizar o cancelar el sistema que se trate.

Etapa intermedia

El propósito de esta etapa es para dar a las Unidades Administrativas la oportunidad de atender las observaciones emitidas en la etapa anterior, con la finalidad de que se ajusten a lo que establece la Política de Gestión de Datos Personales del CENAM y con ello se mantenga la seguridad de los datos personales.

De acuerdo con lo anterior, en esta etapa se desarrollarán las siguientes actividades:

1) Dar asesoría a las Unidades Administrativas que hayan tenido observaciones a su sistema o sistemas de tratamiento de datos personales para que cumpla con las mismas.

2) Otorgar el tiempo necesario para para cumplir con las observaciones y revisar su cumplimiento, máximo serán 3 meses.

3) En caso de incumplimiento parcial o total se deberán emitir nuevas observaciones 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 más próxima, con la finalidad de que manifieste las causas del incumplimiento y se otorgue el tiempo máximo para su cumplimiento.

Etapa final

En el caso que no se hayan emitido observaciones, o bien, habiéndose emitido éstas, se cumplieron satisfactoriamente, se llegará a esta etapa, en la cual se desarrollarán las siguientes actividades:

1) Someter a la aprobación del Comité de Transparencia la implementación, modificación, actualización o cancelación de los sistemas de tratamiento de datos personales.

2) Hacer del conocimiento del Comité de Transparencia la versión final del documento de seguridad.

3) Difundir entre los enlaces de datos personales la versión final del Documento de Seguridad.

Guía de auditoría del Sistema degestión de seguridad de datos personales

Introducción.

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales) establecen una seriede obligaciones a cargo de los sujetos obligados a su cumplimiento, y en el casoconcreto de la Comisión Federal de Competencia Económica (COFECE), el Plan de trabajo integral para la implementación del Sistema de gestión de seguridadde datos personales (SGSDP) establece la generación de un plan de auditoria interno y/o externo para el propio sistema.

Lo anterior, con la finalidad de crear los mecanismos de control del SGSDP en comento, mediante las revisiones y auditorías para evaluar y medir el cumplimiento de las políticas de protección de datos personales a efecto de monitorear y revisar los riesgos que pudieran presentarse.

En ese sentido, existe la obligación y la necesidad de generar la presente guía de auditoría que incluye actividades a desarrollar en el proceso de auditoría delSGSDP, con la finalidad de agilizar su aplicación.

Objetivo.

Proporcionar un instrumento de apoyo que facilite y estandarice las actividadesdel trabajo de auditoría, interno

y/o externo, desde su planeación hasta la presentación del informe de auditoría, así como el seguimiento de las observaciones determinadas.

Esta Guía pretende ser un marco de referencia para monitorear y revisar la eficacia y eficiencia del SGSDP, tomando en cuenta la Política de gestión de datospersonales de la COFECE.

METODOLOGÍA PARA EL DESARROLLO DEL TRABAJO DE AUDITORÍA

El trabajo de auditoría comprende tres etapas: Planeación, Ejecución y Emisióndel Informe.

1. Planeación:

1.1 Planeación General

El auditor llevará a cabo una investigación preliminar del área por auditar, con la finalidad de determinar los objetivos y actividades que se efectuarán, estableciendo los tiempos asignados para la revisión. Dichos aspectos se precisarán en la *Carta Planeación y en el Cronograma de Actividades a Desarrollar.*

La ***Carta Planeación*** incluirá el nombre y cargo del personal participante en laauditoría, la estructura orgánica del área auditada, el marco jurídico aplicable yla posible problemática que pudiese presentarse en el transcurso de la revisión,lo anterior servirá de soporte para la planeación de actividades.

En el ***Cronograma de Actividades a Desarrollar***, se detallan las actividades que se efectuarán desde el inicio hasta su conclusión, y será responsabilidad delpersonal participante en la auditoría vigilar que las actividades determinadas para alcanzar los objetivos y metas de las auditorías, se realicen en tiempo y forma.

Al finalizar la auditoría, el *Cronograma de Actividades a Desarrollar*, se complementará con el tiempo real utilizado y, en su caso, señalar las razones que originaron las variaciones importantes.

1.2 Inicio de la Auditoría

La práctica de auditoría invariablemente se llevará a cabo una vez que se haya notificado el documento denominado ***Aviso de Auditoría***, con las siguientes características:

- Dirigirse al servidor público de mayor jerarquía responsable del área por auditar.
- Estar debidamente fundada y motivada.
- Citar el nombre del personal participante en la auditoría y señalar a un responsable de esta.
- Describir de manera general los alcances de la auditoría.
- Estar firmada por el responsable de la auditoría.

El *Aviso de Auditoría* se entregará a quién va dirigida, obteniendo de puño y letrade éste el acuse de recibo en una copia de la misma (o en su caso se entregaráal servidor público designado para tal efecto).

A) Requerimiento de información

Cuando sea necesario obtener información y documentación vinculada con la auditoría y obre en poder de otra área a la que no se le está practicando la auditoría; así como cuando sea necesario obtener información del área auditada,se procederá a elaborar un requerimiento de información y se deberá entregar la documentación y/o información en la fecha señalada en el requerimiento.

B) Acta de Inicio de Auditoría

En todas las auditorías invariablemente se levantará *Acta de Inicio de Auditoría*,en la que se hará constar lo siguiente:

- Lugar, hora y fecha del acto.
- Nombre de todos los participantes, descripción de la identificación presentada, cargo y unidad administrativa de adscripción.
- Número de control de auditoría, fecha, nombre de la persona a quién va dirigida y del personal participante en la auditoría.
- El apartado de hechos del acta, que describirá la forma en que se presentó el personal participante en la auditoría, con quién se presentaron y el documento con el que se identificaron los que intervienen en el acta. Asimismo, se hará constar la entrega del Aviso de auditoría a quién va dirigida o a la persona designada para atenderla, de la que se obtendrá el acuse de recibo de su puño y letra, así como el sello oficial del área auditada en una copia de la orden de auditoría.
- En el levantamiento del acta se requerirá a la persona con quien se entiende la diligencia, el nombramiento de dos testigos de asistencia; en caso de negativa, el personal participante en la auditoría nombrará a dichos testigos, hecho que quedará asentado en el acta.

También deberán incluirse los siguientes datos de los testigos:

a) Nombre completo.
b) Datos de identificación.
c) Señalamiento de su designación.

- Posteriormente, el personal participante en la auditoría solicitará a la persona con que se entiende la diligencia, si desea agregar algún otro hecho. En caso positivo se le otorgará la palabra y, en caso negativo, se procederá al cierre y término del acta.

C) Oficios Complementarios

Si en el desarrollo de la auditoría se requiere ampliar, reducir o sustituir al personal participante en la auditoría, así como ampliar el tiempo de la revisión o modificar el período y/o el alcance; se hará del conocimiento del área auditadamediante oficio, cumpliendo con las siguientes características:

- Dirigirse al servidor público a quien se giró el Aviso de auditoría.
- Señalar a los auditores que a partir de la fecha del oficio se sustituyen, se incorporen o se retiren de la auditoría y/o describir de manera concreta en qué consiste la ampliación o modificación del alcance y/o el período a revisar.
- Estar firmado por el responsable de la auditoría.
- En un ejemplar de este oficio se recabará el sello del área auditada y la firma de recibido de su Titular.

1.3 Planeación detallada

Esta actividad deberá realizarse previo a la ejecución de la auditoría por el responsable de la auditoría y será sobre el área, obligación o actividad asignadapara su análisis. Esta planeación se documentará en un documento denominado***Marco Conceptual***, considerando los siguientes aspectos:

- Identificación de la auditoría.
- Aspectos por revisar.
- Objetivo que se persigue.
- Obligación o actividad por revisar.
- Procedimientos que se desahogarán durante el desarrollo del trabajo.
- Conclusiones.

La información anterior se obtiene del análisis de las Políticas de Gestión de Datos Personales de la Comisión Federal de Competencia Económica.

Con la planeación detallada, el personal participante en la auditoría podrá identificar el trabajo que ejecutará, además de permitirle el seguimiento de los avances que éste va obteniendo para el establecimiento de los procedimientos por desahogar; delimita las responsabilidades y evita duplicidad de funciones enla auditoría.

En el marco conceptual se deberá especificar cada obligación o actividad por auditar, para que se revise y, en su caso, se adecue el cronograma deactividades por realizar, mismo que contendrá el programa detallado de la revisión.

2. Ejecución del trabajo de Auditoría

En esta la etapa, el auditor deberá obtener evidencia suficiente del área, obligación o actividad que se analiza para contar con elementos suficientes quele permitan determinar el grado de veracidad de la documentación revisada, asícomo la confiabilidad de los documentos examinados, para con ello, estar en posibilidades de emitir una opinión.

La ejecución del trabajo de auditoría se aplicará de manera lógica y sistemáticapara que el auditor reúna elementos informativos suficientes y necesarios para cubrir sus pruebas selectivas, a través de cuatro fases:

- **Recopilación de datos:** El auditor debe allegarse de información y documentación necesaria para su revisión, la cual deberá estar relacionada con el área, obligación o actividad que se analiza a fin de alcanzar el objetivo planteado.

- **Registro de datos:** Se lleva a cabo en los documentos denominados Papeles de Trabajo, en los cuales se incluyen los datos referentes al análisis, comprobación y conclusión de las operaciones examinadas.
- **Análisis de la información:** Consiste en desagregar los elementos de un todo para ser examinados en detalle y obtener un juicio sobre el todo o sobre cada una de sus partes. Cabe señalar que la profundidad del análisis estará en función del objetivo planteado en relación directa con la problemática determinada.
- **Evaluación de los Resultados:** Sólo es posible si se consideran los elementos de juicio suficientes para emitir una opinión, lo cual deberá reflejarse en cédulas de observaciones donde se describirán las irregularidades detectadas, sus causas y efectos, el fundamento legal transgredido y las recomendaciones que el auditor proponga para resolver la problemática.

2.1 Cédulas de trabajo

El procedimiento de auditoría se hará constar en *Cédulas de trabajo*, las cualesdeben contener evidencia de la planeación, ejecución, conclusión, supervisión del trabajo y de los informes que se generen.

La documentación que compruebe una presunta responsabilidad se integrará alexpediente que se envíe al área de responsabilidades o la autoridad competente,sin que en ella se efectúen anotaciones.

Las reglas generales para la elaboración de los papeles de trabajo son:

- Identificar el área, obligación o actividad revisada, la fecha de elaboración de la cédula, nombre y firma del auditor que la elaboró y firma del responsable de la auditoría como evidencia de la supervisión que realizó.
- Deben ser completos y suficientemente detallados de tal manera que permita su inmediata comprensión sin dificultad alguna y sin perder claridad.
- Contener fuentes de información, referencias, conclusión y notas.
- Ser pulcros, legibles y ordenados lógicamente.

Al concluir la revisión, los papeles de trabajo formarán parte del expediente de auditoría, por lo que deben integrarse en legajos debidamente ordenados de manera lógica y ser resguardados en el archivo documental de la COFECE.

3. Emisión del Informe

El informe debe ser oportuno, completo, exacto, objetivo, claro, conciso y útil.

3.1 Cédula de observaciones

Es el documento en el que se concentrarán los resultados en los que se determinen situaciones irregulares o susceptibles de mejora.

Los auditores que participaron en la revisión presentarán y comentarán las cédulas de observaciones con los servidores públicos responsables del área auditada, a través de una reunión, misma que deberá documentarse en un ***Actade Cierre***, dos días antes de la presentación formal del informe de auditoría.

De esa reunión podrán obtenerse elementos adicionales que ratifiquen lairregularidad, así como las causas que las provocan, o bien, que justifiquen las causas de las situaciones irregulares o susceptibles de mejora.

Asimismo, se acordará con los servidores públicos responsables las recomendaciones que deberán atender, incluyendo aquellas acciones que permitan dar solución, no solo a la irregularidad detectada, sino a la problemática esencial que ocasionan las irregularidades.

Las *cédulas de observaciones* contendrán un apartado en el que el o los servidores públicos responsables del área auditada indicarán el día, mes y año en que se comprometen a atender las recomendaciones, **sin exceder el plazode cuarenta días hábiles**.

En este mismo apartado se anotará el nombre y cargo de los servidores públicosresponsables, así como del responsable de la auditoría, quienes deberán firmarla cédula de observaciones.

No obstante, cuando los servidores públicos responsables se negaran a firmarlas, se asentará en el *Acta de Cierre* dicha situación y se harán constar losmotivos por los cuales no fueron firmadas las observaciones.

Si derivado de la investigación se determinan irregularidades que conlleven responsabilidades, el auditor responsable de la revisión informará al Órgano Interno de Control anexando el informe correspondiente y la documentación quela sustenta.

Para que las recomendaciones incidan favorablemente en la mejora del complimiento de las obligaciones o actividades, el auditor debe considerar los siguientes aspectos:

- Definir la problemática observada.
- Identificar las causas reales que provocaron las irregularidades.
- Visualizar las repercusiones a corto y mediano plazo que ocasionan las irregularidades en las actividades, obligaciones o áreas responsables que se interrelacionan con el aspecto auditado.

- Plantear recomendaciones acordadas con el área auditada, que solucionen en un tiempo razonable las causas reales de las irregularidades y eviten la incidencia en otras actividades u obligaciones relacionadas con el área o aspecto auditado.

3.2 Informe de Auditoría

Una vez comentadas las observaciones determinadas y firmadas por los responsables de su atención, se deberá comunicar al titular del área auditada los resultados a través del documento denominado ***Informe de Auditoría***.

El *Informe de Auditoría* debe contener la declaración formal del auditor de haberdesarrollado su trabajo de conformidad con los papeles de trabajo.

El informe constará de cinco elementos:

A) Oficio de envío del informe ejecutivo

Es el documento mediante el cual se hace oficial el envío del informe al Presidente del Comité de Transparencia y al Titular del área auditada. El objetivoprincipal de este informe es que de forma resumida se den a conocer las observaciones determinadas, describiendo de manera clara y precisa los principales problemas que enfrenta el área auditada, así como las obligaciones y/o actividades analizadas, las situaciones irregulares o susceptibles de mejora,su origen, repercusiones y efectos, tal como se estableció en las cédulas de observaciones.

B) Carátula del informe

Presenta un resumen de los datos más importantes de la auditoría para su fácilidentificación; contiene entre otros aspectos, el nombre del área auditada, obligación o actividad auditada, número de control de la auditoría, fechas de inicio y término, fecha de discusión de observaciones, nombre del personal participante en la auditoría y del responsable de la auditoría.

C) Índice

Se numeran los capítulos que integran el informe, señalando el número de la página donde se localiza cada apartado.

D) Cuerpo del informe

Se dan a conocer los resultados de los trabajos efectuados de manera resumida;y se estructura de la siguiente manera:

- **Antecedentes:** Se anotarán las causas que originaron la revisión, las principales funciones u operaciones del área evaluada y cualquier otro elemento que sea necesario mencionar.
- **Período:** Indica el lapso en que se realizaron los trabajos de auditoría.
- **Objetivo:** Los logros que se propusieron alcanzar con la revisión.

- **Alcances:** Señala el área evaluada, obligaciones y actividades revisadas.
- **Resultados del trabajo desarrollado:** En este apartado se describen los aspectos relevantes identificados durante la auditoría, pero no como una transcripción o síntesis de las observaciones determinadas ni la mención de las situaciones irregulares o susceptibles de mejora específicas o particulares.

  Los resultados incluidos en el informe deben corresponder a problemas definidos con precisión y que sean el origen de las situaciones irregulareso susceptibles de mejora, tal y como fueron plasmados en las cédulas deobservaciones, haciendo hincapié en las repercusiones dentro de las actividades, obligaciones o áreas auditadas.

  Además, deben proporcionar información valiosa para la toma de decisiones por parte de los servidores públicos responsables de atenderlas; por ello, el auditor vinculará las diferentes desviaciones paramostrar cómo, en su conjunto, repercuten y afectan la planeación,programación y ejecución de los programas y consecuentemente el logrode los objetivos.

  El objetivo del informe va más allá de evidenciar los errores o deficiencias,también destaca los aciertos que fueron identificados. En este sentido, debe hacerse referencia a los elementos de éxito que permitieron el logrode los objetivos.
- **Conclusión y recomendaciones:** Como importante es señalar las deficiencias más significativas, también lo es promover acciones que conlleven su solución; por ello, dentro del informe de auditoría se incluirán las conclusiones y recomendaciones generales.

Debido a que en las *Cédulas de observaciones* quedaron escritas recomendaciones específicas acordadas con los servidores públicos responsablesde atenderlas, la recomendación general debe estar planteada de tal manera que aporte elementos para la toma de decisiones en la planeación, programación, organización, ejecución, control y evaluación de las obligacionesasignadas al área auditada.

E) Observaciones

Se incluyen todas las *Cédulas de observaciones* comentadas y firmadas como evidencia de la formalización de su envío al área auditada.

SEGUIMIENTO DE RECOMENDACIONES

El seguimiento de las recomendaciones se refiere a la revisión y comprobación de las acciones realizadas por el área auditada para atender en tiempo y formalas recomendaciones preventivas y correctivas sugeridas en la auditoría, a fin deque se corrijan las situaciones irregulares o susceptibles de mejora y se evite surecurrencia.

A) Cédulas de seguimiento

Manifiestan el avance en la atención de las situaciones irregulares o susceptiblesde mejora detectadas durante la auditoría, en ellas se verifica que las recomendaciones hechas por el auditor y las acciones implantadas por el área auditada hayan sido aplicadas y que permitan la solución de la problemática o, en su caso, el avance en su solución.

Asimismo, las cédulas deben contener, además de la identificación de laauditoría, los siguientes datos:

- La observación a la cual se da seguimiento.
- Las acciones realizadas por el área auditada para dar solución a la problemática planteada.
- El juicio u opinión del auditor para considerar solventada o no la irregularidad.
- En caso de no estar solventada la observación, el replanteamiento que propone el auditor, mediante medidas correctivas y/o preventivas para solventarlas.
- La fecha compromiso en la que el área auditada considera resolver las irregularidades.
- Al igual que las cédulas de observaciones, las de seguimiento deben ser comentadas con el responsable del área auditada, hasta dos días antes de quedar plasmadas en el informe de auditoría.

El plazo máximo para la atención de observaciones y/o recomendaciones, será de **cuarenta días hábiles** contados a partir de la entrega del informe de auditoría al titular del área auditada.

En caso de presentarse circunstancias que desfasen los períodos de atención delas observaciones y/o recomendaciones, será necesario que los servidores públicos responsables de las áreas auditadas avisen sobre tal situación de manera inmediata y por escrito al responsable de la auditoría, quien podrá autorizar una prórroga en casos debidamente justificados y por única vez.

La ***Solicitud de prórroga*** deberá ser solicitada por escrito, por el responsable del área auditada, con cinco días hábiles de anticipación a la fecha límite para laatención de observaciones, siendo necesario que se expliquen claramente las razones por las cuales se retrasará la entrega de información de que se trate y el tiempo que se requerirá para su atención.

El responsable de la auditoría deberá analizar si cada solicitud está debidamentemotivada y si procede otorgar la prórroga solicitada.

Las solicitudes de prórroga que se tramiten con posterioridad al plazo establecidoen este párrafo no surtirán efecto alguno.

B) Oficio de envío de resultados del seguimiento

Una vez concluidas las cédulas de seguimiento, mediante oficio emitido por el responsable de la auditora se informarán los resultados determinados en el seguimiento al Titular de la Unidad auditada y a las instancias que en cada casose requiera.