



SALUD
SECRETARÍA DE SALUD



Instituto Nacional de
Medicina Genómica



Dirección General
Unidad de Transparencia

MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

El artículo 30, fracción V, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, establece que entre los mecanismos que se deberán adoptar para cumplir con el principio de responsabilidad, se encuentra el poner en práctica un programa de capacitación y actualización de las personas servidoras públicas del Instituto Nacional de Medicina Genómica (INMEGEN) sobre las obligaciones y demás deberes en materia de protección de datos personales.

Al respecto, el artículo 33, fracción VIII, de la Ley General, dispone diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

En ese sentido, el artículo 35, fracción VI y VII, 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 y el programa general de capacitación.

Para dichos efectos, el artículo 84, fracción VII de la Ley General, establece que el Comité de Transparencia tendrá la función de:

- Establecer programas de capacitación y actualización para las personas servidoras públicas en materia de protección de datos personales.

Para ello, el INMEGEN contará con una persona Enlace de Capacitación ante la Dirección General de Capacitación del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), a lo cual, coadyuvará con la Unidad de Transparencia y con la Red convirtiéndose en interlocutora y aliada entre el INMEGEN y el INAI, con el propósito de fortalecer la cultura de transparencia, acceso a la información y protección de datos personales.

En ese sentido, el artículo 64 de los Lineamientos Generales de protección de datos personales para el sector público establece que el responsable deberá diseñar e implementar programas a corto, mediano y largo plazo que tengan por objeto capacitar a los involucrados internos y externos en su organización, considerando sus roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales y el perfil de sus puestos.

En el diseño e implementación de los programas de capacitación a que se refiere el párrafo anterior del presente artículo, el responsable deberá tomar en cuenta lo siguiente:

- I. Los requerimientos y actualizaciones del sistema de gestión;
- II. La legislación vigente en materia de protección de datos personales y las mejores prácticas



- relacionadas con el tratamiento de éstos;
- III. Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales, y
- IV. Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad.

Asimismo, se debe considerar que las áreas responsables tendrán que establecer, actualizar y mejorar las actividades necesarias para las medidas de seguridad de los tratamientos de datos personales.

El monitoreo y reporte de las actividades generadas se llevará a cabo de manera periódica por la Unidad de Transparencia, a fin de mantener en conocimiento del Comité de Transparencia lo relativo al tratamiento de los datos personales a cargo de la Institución. De igual manera, se deberá realizar un análisis constante de las posibles amenazas y/o vulneraciones que se pudieran presentar en los sistemas, o bien, lugares físicos del Instituto Nacional de Medicina Genómica.

En ese sentido, el Instituto desarrollará el cumplimiento de dicha obligación a través de los siguientes mecanismos:

A. MECANISMOS DE MONITOREO Y SUPERVISIÓN.

	Sí	No
1. Se definieron las funciones, obligaciones y cadena de mando de cada servidor público que trata datos personales, por unidad administrativa.	<input type="checkbox"/>	<input type="checkbox"/>
2. 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 específicas o adicionales a las previstas en la LGPDPSO y los Lineamientos Generales, y se ha definido la procedencia de su implementación		
3. Se ha comunicado a cada servidor público sus funciones, responsabilidades, obligaciones y cadena de mando con relación al tratamiento de datos personales que efectúa.	<input type="checkbox"/>	<input type="checkbox"/>



<p>4. Se ha elaborado un inventario con la información básica de cada tratamiento de datos personales que se realiza en el INMEGEN a lo previsto en el artículo 33, fracción III, de la Ley General, el cuál considera:</p> <ul style="list-style-type: none"> • El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales; • Las finalidades de cada tratamiento de datos personales; • El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no; • El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales; • La lista de servidores públicos que tienen acceso a los sistemas de tratamiento; • En su caso, el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable, y • En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que las justifican. 	<input type="checkbox"/>	<input type="checkbox"/>
<p>5. En el inventario de datos personales se tomó en cuenta el ciclo de vida de los datos personales, conforme a lo siguiente:</p> <ul style="list-style-type: none"> • La obtención de los datos personales; • El almacenamiento de los datos personales; • El uso de los datos personales conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin; • La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen; • El bloqueo de los datos personales, en su caso, y • La cancelación, supresión o destrucción de los datos personales. 	<input type="checkbox"/>	<input type="checkbox"/>



<p>6. Se ha realizado el análisis de riesgo, considerando el siguiente procedimiento:</p> <p>A. Se analizan los posibles riesgos existentes a través de cuestionarios, revisión de la infraestructura tecnológica, así como el cumplimiento a la normativa en materia de datos personales.</p> <p>B. Detectadas las posibles vulnerabilidades y amenazas, la unidad administrativa establece controles de seguridad a fin de mitigar las mismas.</p> <p>C. Se efectúa un análisis de brecha que permita identificar y definir controles de seguridad que sean necesarios.</p> <p>D. La unidad administrativa responsable y el Comité de Transparencia realizan una ponderación de los riesgos a fin de determinar y priorizar las medidas de seguridad a implementar, tomando en cuenta las consecuencias de una probable vulneración, el número de titulares afectados y el riesgo cuantitativo o cualitativo.</p> <p>E. Se elabora un plan de trabajo en el cual se identifique a los responsables de implementar dichas acciones.</p>	<input type="checkbox"/>	<input type="checkbox"/>
<p>7. Las áreas responsables de los tratamientos ha realizado una bitácora de vulneraciones que se lleguen a sufrir, el cual debe contener:</p> <ol style="list-style-type: none"> 1. Descripción de la vulneración sufrida, datos afectados y número estimado de titulares en riesgo, 2. Fecha en que ocurrió, 3. Motivo que la generó, 4. Acciones implementadas para su solución y respuesta, documentando las gestiones realizadas. 	<input type="checkbox"/>	<input type="checkbox"/>

B. PROGRAMA GENERAL DE CAPACITACIÓN.

Con relación al programa de capacitación, la fracción VIII del artículo 33 de la LGPDPPSO señala que, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

En ese sentido, de acuerdo con la fracción VII del artículo 35 de la LGPDPPSO, el programa de capacitación forma parte del documento de seguridad, el cual se encuentra previsto de conformidad con las acciones previstas por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, así como la propuesta de capacitación definida por las unidades administrativas que integran el INMEGEN.





SALUD
SECRETARÍA DE SALUD



Instituto Nacional de
Medicina Genómica



Dirección General
Unidad de Transparencia

En tal entendido, en el diseño e implementación del programa de capacitación, se toma en cuenta lo siguiente:

- I. Los requerimientos y actualizaciones del sistema de gestión;
- II. La legislación vigente en materia de protección de datos personales y las mejores prácticas relacionadas con el tratamiento de éstos;
- III. Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales, y
- IV. Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad.

Así mismo, con la finalidad de que las personas servidoras públicas del Instituto conozcan sus obligaciones y, estén en posibilidad de dar cumplimiento a los principios y deberes en materia de protección de datos personales, la capacitación se llevará a cabo en dos vertientes: básica y especializada.

- **Capacitación básica**

El propósito de esta capacitación es que las personas conozcan los aspectos teóricos, conceptuales y normativos fundamentales en materia de protección de datos personales.

Se considerará el curso denominado Introducción a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, mismo que será OBLIGATORIO, para todas las personas servidoras públicas del INMEGEN e integrantes del Comité de Transparencia.

- **Capacitación especializada**

La capacitación especializada será determinada en función de las necesidades que se pretendan cubrir por cada una de las áreas que realizan tratamientos de datos personales.

Es importante mencionar, que el Instituto Nacional de Medicina Genómica se sujeta al Programa de Capacitación en Transparencia y Acceso a la Información, Protección de Datos Personales que imparte el Instituto Nacional de Acceso a la Información y Protección de Datos Personales (INAI) en relación con las siguientes capacitaciones:

- Introducción a la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados.
- Clasificación de la Información y Prueba de Daño.
- Fundamentos del Documento de Seguridad en Materia de Protección de Datos Personales.
- Elaboración del Documento de Seguridad en Materia de Protección de Datos Personales.
- Aviso de Privacidad en el Sector Público.
- Sistema de Gestión de Seguridad de Datos Personales en el Sector Público.
- Auditorías Voluntarias en Materia de Protección de Datos Personales en el Sector Público.



SALUD
SECRETARÍA DE SALUD



Instituto Nacional de
Medicina Genómica



Dirección General
Unidad de Transparencia

- Esquemas de Mejores Prácticas en Materia de Protección de Datos Personales en el Sector Público.

En el caso particular del INMEGEN, el desarrollo del programa de capacitación está a cargo de la Unidad de Transparencia, el cual deberá ser revisado y reestructurado periódicamente, de manera anual, cuyos objetivos principales son los siguientes:

- La participación y certificación de los involucrados en los tratamientos de datos personales, en los cursos de capacitación ofertados por el Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (INAI)
- La identificación a través de la aplicación de un cuestionario interno para la detección de necesidades de capacitación en materia de protección de datos personales.
- La identificación de aquellas necesidades de capacitación derivadas de los análisis de riesgos y de brecha que impacten en la protección de datos personales.

MEDIDAS ADMINISTRATIVAS:

Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger datos personales. Por ello se definen, se establecen y mantienen de manera enunciativa lo siguiente en 3 diferentes modalidades:

Medidas de seguridad físicas: acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.

Medidas de seguridad administrativas: introduce políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales.

Medidas de seguridad técnicas: conjunto de acciones y mecanismos que se valen de la tecnología relacionada con el hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento.