DOCUMENTO DE SEGURIDAD

INSTITUTO NACIONAL DE MEDICINA GENÓMICA

Junio 2021

Contenido

GLOSARIO

INMEGEN	Instituto Nacional de Medicina Genómica
LGPDPPSO	Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
LinGPDPPSP	Lineamientos Generales de Protección de Datos Personales para el Sector Público.

Introducción

El INMEGEN es un organismo descentralizado de la Administración Pública Federal, con personalidad jurídica y patrimonio propios, con autonomía de decisión técnica, operativa y administrativa en los términos de la Ley de los Institutos Nacionales de Salud y la Ley Federal de las Entidades Paraestatales, agrupado en el Sector coordinado por la Secretaría de Salud, creado mediante decreto presidencial publicado en el Diario Oficial de la Federación, el 20 de julio del 2004, que tiene por objeto, en el campo de la medicina genómica, la investigación científica, la formación y capacitación de recursos humanos especializados, el desarrollo de tecnología y la vinculación con la industria para el desarrollo de productos y servicios de base genómica, y cuyo ámbito de acción comprende todo el territorio nacional.

El 26 de enero del 2017 se expidió la LGPDPPSO la cual tiene como objetivo establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales que estén en posesión de los sujetos obligados, de cuyo artículo primero se desprende la calidad de sujeto obligado del INMEGEN, al ser una entidad de la Administración Pública Federal que lleva a cabo el tratamiento de datos personales y, por ello, debe observar lo dispuesto por dicho instrumento normativo en el tratamiento de datos personales que lleve a cabo.

Asimismo, la LGPDPPSO detalla el alcance y los procedimientos para el ejercicio de los cuatro derechos que el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos reconoce a los titulares de los datos personales: acceso, rectificación, cancelación y oposición (derechos ARCO), y reconoce uno más, el de portabilidad.

En ese sentido, el 26 de enero del 2018, se publicaron los LinGPDPPSP de Protección de Datos personales para el Sector Público, derivado de lo anterior, a partir de la publicación de dichos instrumentos jurídicos, el INMEGEN, adquirió el carácter de “Responsable” con el deber de tratar dichos datos conforme a los principios (licitud, lealtad, información, consentimiento, finalidad, proporcionalidad, calidad y responsabilidad) y (confidencialidad y seguridad).

Estos principios, deberes y derechos imponen una serie de obligaciones para los sujetos regulados por la LGPDPPSO, que tienen como finalidad que el tratamiento se realice de manera tal que se garantice la protección de los datos personales, con el objeto de respetar el derecho a la autodeterminación informativa de los titulares.

En específico, con relación al deber de seguridad, el artículo 31 de la LGPDPPSO señala que el Responsable del tratamiento deberá establecer y mantener medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos

contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

Por su parte, el artículo 35 de la LGPDPPSO establece como una obligación la elaboración de un documento de seguridad, que describa y de cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

En ese sentido, en cumplimiento a las obligaciones antes descritas, a continuación, se presenta el documento de seguridad del INMEGEN con los elementos informativos que establece la normativa de la materia.

I. Inventario de datos personales y de los sistemas de tratamiento

La LGPDPPSO en sus fracciones I y III del artículo 33 establece la obligación elaboración de contar con un inventario de datos personales y de los sistemas de tratamiento para la implementación de medidas de seguridad para la protección de los datos personales, mismo que forma parte del documento de seguridad; los inventarios de datos personales forman parte integral del presente documento.

Sobre el particular, el INMEGEN elaboró los inventarios de los distintos tratamientos de datos personales que realiza, identificando los elementos informativos, basados en el ciclo de vida de cada uno de éstos; de conformidad con lo dispuesto en los artículos 58 y 59 de los LinGPDPPSP de Protección de Datos Personales para el Sector Público.

No.	Áreas	No. Inventarios Entregados	Nombre del Tratamiento	Finalidades
1	Dirección de Investigación	2	Investigación	Proyectos de Investigación
				Servicios de Laboratorio
2	Dirección de Administración	8	Administración de capital humano	Contrataciones de personal
				Emisión de credencial
			Administración de recursos financieros	Pago a proveedores
				Pago recursos de terceros
			Administración de recursos materiales	Resguardo de inventario
				Entrada y Salida de Personal
				Tarjetón vehicular
				Procedimientos de Contratación
3	Dirección de Vinculación y Desarrollo Institucional	9	Dirección estratégica	Trámite de solicitudes de acceso a la información pública y recursos de revisión
				Ejercicio de derechos ARCO y recursos de revisión
			Asuntos institucionales (internos, externos e internacionales)	Tratamiento de Información para miembros de la Junta de Gobierno
				Coinventores de patentes o derechos de autor
				Autenticación licenciatarios y socios estratégicos
				Identificación de clientes de servicios de

				consultoría
				Entrevistas, encuestas, estudios de mercado
			Asuntos jurídicos	Cumplimiento a requerimientos de autoridades
				Contratos, convenios y acuerdos
4	Dirección de Desarrollo Tecnológico	1	Soporte tecnológico	Mesa de ayuda, clúster institucional
5	Dirección de Enseñanza y Divulgación	3	Enseñanza	Eventos académicos
				Estudiantes y egresados
				Estudiantes y egresados ME
Total		**23**		

II. Funciones y obligaciones de las personas que traten datos personales

En cumplimiento a la fracción II del artículo 33 de la LGPDPPSO, el INMEGEN, identifica las funciones y obligaciones del personal que lleva a cabo el tratamiento de datos personales de la siguiente manera:

1. Atendiendo lo dispuesto en la LGPDPPSO y los LinGPDPPSP, mismos que se encuentran asociados con cada una de las áreas responsables de su cumplimiento.

2. Atendiendo a los servidores públicos que realizan el tratamiento, área al cual se encuentra adscrito y finalidad de dicho tratamiento.

El INMEGEN cuenta con roles y funciones del personal con respecto al tratamiento y protección de los datos personales, los cuales se describan en el presente apartado de manera general y particular, con independencia de que el inventario de datos personales funja como una bitácora donde quedan establecidos los responsables, encargados y usuarios de los datos personales.

Cabe señalar que el Comité de Transparencia es el área responsable de dar a conocer a los servidores públicos del INMEGEN el Programa de Protección de Datos Personales, a fin de que el personal conozca sus funciones las cuales se encuentran definidas en la legislación y normatividad que rige el actuar del Instituto, por lo cual, para efectos del presente documento de seguridad, el marco normativo de referencia se encuentra establecido en el Manual de Organización Específico del INMEGEN.

En ese sentido, resulta importante señalar que la legislación y normatividad aplicable al INMEGEN que define las atribuciones, responsabilidades, autoridades, funciones y obligaciones al interior de la organización, se encuentra disponible de manera actualizada en el apartado Normatividad de la Plataforma Nacional de Transparencia disponible en el vínculo siguiente: https://tinyurl.com/yjrqc49r.

Adicionalmente, a fin de identificar la relación de las funciones por unidades administrativas del INMEGEN y el marco normativo aplicable a dicha gestión, deberá consultarse el Manual de Organización Específico del INMEGEN, el cual se encuentra disponible en el apartado de normatividad de la página del INMEGEN, o directamente en el vínculo siguiente: https://www.inmegen.gob.mx/media/filer_public/61/e3/61e33985-d4eb-47e9-8e25-8335ba48e1c1/mo e-inmegen-2016_1_1.pdf

III, IV y V. Análisis de riesgos, Análisis de brecha y Plan de Trabajo

Dentro de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, el análisis de riesgo, análisis de brecha y plan de trabajo, forman parte del documento de seguridad del INMEGEN de conformidad con lo dispuesto en los artículos 32, 35 fracciones IV, V y V de la LGPDPPSO así como 60, 61 y 62 de los LinGPDPPSP.

Análisis de riesgo

Al efecto, el análisis de riesgo realizado por el INMEGEN, prevé aquellos atinentes a: 1) Infraestructura tecnológica (software y hardware), 2) Hábitos de seguridad del personal, 3) Inventarios de tratamiento de datos personales y 4) Cumplimiento de obligaciones normativas en materia de datos personales.

En ese sentido, el cumplimiento previsto en los artículos 33 fracción IV de la LGPDPPSO así como 60 de los LinGPDPPSP, se prevé de la siguiente manera:

Elemento requerido	Fuente
Amenazas y vulnerabilidades existentes. Art. 33, fracción IV, de la LGPDPPSO	• Infraestructura tecnológica; • Hábitos de seguridad del personal; • Inventarios de tratamientos de datos personales, y • Cumplimiento de obligaciones normativas en materia de datos personales.
Recursos involucrados en el tratamiento de datos personales. Art. 33, fracción IV, de la LGPDPPSO	• Infraestructura tecnológica • Inventarios de tratamientos de datos personales.
Requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico. Art. 60, fracción I, de los LinGPDPPSP	• Cumplimiento de obligaciones normativas en materia de datos personales.
El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida. Art. 60, fracción II, de los LinGPDPPSP	• Inventarios de tratamientos de datos personales.
El valor y exposición de los activos involucrados en el tratamiento de los datos personales Art. 60, fracción III, de los LinGPDPPSP	• Hábitos de seguridad del personal.
Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida.	• Ponderación de riesgos.

Elemento requerido	Fuente
Art. 60, fracción IV, de los LinGPDPPSP	
El riesgo inherente a los datos personales tratados. Art. 32, fracción I, de la LGPDPPSO	• Inventarios de tratamientos de datos personales.
La sensibilidad de los datos personales tratados. Art. 32, fracción II, de la LGPDPPSO	• Inventarios de tratamientos de datos personales.
El desarrollo tecnológico. Art. 32, fracción III, de la LGPDPPSO	• Infraestructura tecnológica.
Las posibles consecuencias de una vulneración para los titulares. Art. 32, fracción IV, de la LGPDPPSO.	• Ponderación de riesgos.
Las transferencias de datos personales que se realicen. Art. 32, fracción V, de la LGPDPPSO	• Inventarios de tratamientos de datos personales.
El número de titulares. Art. 32, fracción VI, de la LGPDPPSO	• Ponderación de riesgos.
Las vulneraciones previas ocurridas en los sistemas de tratamiento. Art. 32, fracción VII, de la LGPDPPSO	• Reportes de vulneraciones al Comité de Transparencia.
El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión. Art. 32, fracción VIII, de la LGPDPPSO	• Ponderación de riesgos.

Con la finalidad de identificar los riesgos inherentes al tratamiento de datos personales así como el establecimiento de controles de seguridad, el INMEGEN lleva a cabo el siguiente procedimiento:

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.

B. Detectadas las posibles vulnerabilidades y amenazas, la unidad administrativa establece controles de seguridad a fin de mitigar las mismas.

C. Se efectúa un análisis de brecha que permita identificar y definir controles de seguridad que sean necesarios.

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.

E. Se elabora un plan de trabajo en el cual se identifique a los responsables de implementar dichas acciones.

La evidencia de la implementación de los análisis forman parte de los elementos que brindan el contexto para la identificación de los riesgos, basado en las etapas siguientes:

1. Contexto de la organización (basado en los elementos factores previstos por el artículo 32 de la LGPDPPSO).

2. Identificación del riesgo.

3. Análisis del riesgo.

4. Administración del riesgo.

5. Tratamiento del riesgo.

Análisis cuyos resultados se implementan como mejorar en los mecanismos de monitoreo y seguimiento de las medidas de seguridad, o en su defecto, se incorporan dentro del Plan de Trabajo.

El análisis de riesgos se realiza cuando menos una vez cada dos años de manera general, tomando en consideración de manera genérica todos los tratamientos de datos personales. No obstante, las unidades administrativas pueden realizar análisis de riesgos sobre sus propios tratamientos, los cuales son susceptibles de ser reconocidos como parte integrante del presente documento de seguridad.

Análisis de brecha

Para efectos del presente documento, el análisis de brecha solamente comprenderá los riesgos que conforme el análisis realizado sea necesario tratar, así como aquellos otros supuestos que, en términos de la LGPDPPSO se requiera dicho análisis.

En ese sentido, a fin de cubrir con los requerimientos previstos por el artículo 61 de los LinGPDPPSP, para la realización del análisis de brecha se deberán considerar las medidas de seguridad existentes y efectivas; las medidas de seguridad faltantes, y la existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente; en el que se identifican los siguientes elementos:

- Confirmación de la existencia de la brecha.
- Confirmación de que la brecha es gestionable, o en su caso, que se han implementado acciones para su contención.
- Identificación de alternativas de corto plazo para su atención.
- Elaboración de un cronograma que defina las principales actividades, resultados y responsables para que la brecha pueda ser atendida.

Plan de Trabajo

El plan de trabajo define las principales acciones a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer. Lo anterior, considerando los recursos designados; el personal interno y externo en su organización y las fechas compromiso para la implementación de las medidas de seguridad nuevas o faltantes.

No obstante, dentro del Plan de Trabajo también podrá agregarse cualquier actividad que resulte como requisito para la mejora institucional que se traduzca de manera directa o indirecta en la protección de datos personales.

VI. Mecanismos de monitoreo y revisión de las medidas de seguridad

Mecanismos de monitoreo

En cumplimiento a lo previsto en el artículo 35 fracción VI de la LGPDPPSO y 63 de sus LinGPDPPSP, el INMEGEN lleva a cabo la revisión del cumplimiento de las políticas internas relacionadas con el tratamiento de datos personales.

Para tal efecto, de conformidad con el Plan de Trabajo establecido cada una de las unidades administrativas, deberá remitir la evidencia que sustente las acciones realizadas para su cumplimiento en el mes de noviembre, a efecto de informar dichos avances al Comité de Transparencia tales como:

1. Revisar y en su caso actualizar los procesos involucrados en el tratamiento de datos personales
2. Revisar y en su caso actualizar los avisos de privacidad, funciones y obligaciones del personal y los inventarios de datos personales, según corresponda.
3. Evaluar si hubo cambios en las amenazas, vulnerabilidades o impacto de los riesgos relacionados con las modificaciones a la normativa, para actualizar los análisis de riesgos, análisis de brecha y plan de trabajo
4. Revisar y en su caso adecuar los sistemas de tratamiento para cumplir con los cambios normativos.
5. Monitoreo del entorno físico (personal de vigilancia, control de acceso, control de asistencia, circuito cerrado)
6. Monitoreo del entorno electrónico (verificaciones área informática)
7. Actualización del plan de trabajo
8. Revisión de avances del plan de trabajo
9. Actualización de tecnología
10. Vulneraciones a la seguridad de datos personales.

Para tales efectos, cada unidad administrativa define les medidas de seguridad en atención a las responsabilidades y autoridades inherentes a cada puesto, y, los elementos establecidos previamente constituyen controles generales adicionales a los ya implementados por cada una de las áreas administrativas.

No obstante, cuando derivado de los resultados del análisis de riesgos, del análisis de brecha y del plan de trabajo reconocidos en el presente documento de seguridad se desprendan actividades o compromisos específicos, la unidad de transparencia dará seguimiento a cada uno de los compromisos reconocidos. Adicionalmente, con independencia de lo establecido por el presente documento de seguridad, se podrá establecer un periodo de 3 a 6 meses para la evaluación y actualización del documento de seguridad, periodo durante el cual, se mantendrá vigente la versión disponible.

Las mejoras y actualizaciones del documento de seguridad deberán ser comunicadas a todo el personal del INMEGEN dentro de los 6 meses siguientes a que sea presentado ante el Comité de Transparencia.

Mecanismos de supervisión o revisión

Actualmente no se han llevado a cabo auditorías específicas en materia de protección de datos personales a los tratamientos del INMEGEN. Al respecto, se prevé la realización de una auditoría anual ya sea por terceros según la disponibilidad presupuestal, por solicitud al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales o bien, por personal del Instituto.

El programa anual de auditoría, así como la realización de las mismas, será determinado por el Comité de Transparencia en el Programa de Protección de Datos Personales del INMEGEN, conforme a los términos de referencia que se determinen para tal efecto dentro de la institución que podrán tomar como referencia el procedimiento de auditorías voluntarias por parte del INAI, sin perjuicio que, de considerarse conveniente en el marco de la mejora institucional, se solicite ante dicho Instituto la práctica de dicho ejercicio.

VII. 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.

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.

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.

En tal entendido, el Programa General de Capacitación del INMEGEN, se establece a través de este apartado con el objetivo general que se señala a continuación:

Objetivos de Capacitación

El personal que integra el INMEGEN deberá estar capacitado en su totalidad en materia de protección de datos personales en posesión de sujetos obligados conforme a los criterios siguientes:

- Inducción proporcionada bajo la coordinación de la Unidad de Transparencia del INMEGEN con relación a la operación y mantenimiento de su Sistema de Gestión y la operación del documento de seguridad dentro del año posterior a su ingreso.

- Cursos que proporciona el INAI, dentro de los dos años posteriores a su ingreso.

Avisos de privacidad.

Con fundamento en los artículos 27 y 28 de la LGPDPPSO, los relativos a sus Lineamientos y los artículos 11, 14, 15, 16 y 19 de los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales (Lineamientos de Portabilidad), los responsables tienen la obligación de elaborar Avisos de Privacidad, de los cuales el INMEGEN ha elaborado los siguientes:

No.	Áreas	No. Inventarios Entregados	Nombre del Tratamiento	Finalidades	Aviso de Privacidad Integral	Aviso de Privacidad Simplificado
1	Dirección de Investigación	2	Investigación	Proyectos de Investigación	X	X
				Servicios de Laboratorio	X	X
2	Dirección de Administración	8	Administración de capital humano	Contrataciones de personal	X	X
				Emisión de credencial		
			Administración de recursos financieros	Pago a proveedores	X	X
				Pago recursos de terceros		
			Administración de recursos materiales	Resguardo de inventario	X	X
				Entrada y Salida de Personal	X	X
				Tarjetón vehicular	X	X
				Procedimientos de Contratación	X	X
3	Dirección de Vinculación y Desarrollo Institucional	9	Dirección estratégica	Trámite de solicitudes de acceso a la información pública y recursos de revisión	X	X
				Ejercicio de derechos ARCO y recursos de revisión	X	
			Asuntos institucionales (internos, externos e	Tratamiento de Información para	X	X

			internacionales)	miembros de la Junta de Gobierno		
				Coinventores de patentes o derechos de autor	X	
				Autenticación licenciatarios y socios estratégicos		
				Identificación de clientes de servicios de consultoría		
				Entrevistas, encuestas, estudios de mercado		
			Asuntos jurídicos	Cumplimiento a requerimientos de autoridades	X	X
				Contratos, convenios y acuerdos		
4	Dirección de Desarrollo Tecnológico	1	Soporte tecnológico	Mesa de ayuda, clúster institucional	X	X
5	Dirección de Enseñanza y Divulgación	3	Enseñanza	Eventos académicos	X	X
				Estudiantes y egresados	X	X
				Estudiantes y egresados ME	X	X
Total		**23**				

Actualización del documento de seguridad

En cumplimiento a lo dispuesto por el artículo 36 de la LGPDPPSO, se establece la actualización del presente documento, cuando se lleve a cabo la creación de un nuevo sistema o base de datos que implique el tratamiento de datos personales, el titular de la unidad administrativa deberá dar aviso por escrito al titular de la Unidad de Transparencia así como remitir la información correspondiente para su inclusión en el Inventario del Sistema de Tratamiento de Datos del Instituto.

Aunado a lo anterior, el INMEGEN, determinará la actualización del presente documento de conformidad con las herramientas metodológicas emitidas por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Cabe señalar que una vez que sufra alguna actualización el presente Documento de Seguridad, la misma será sometida a consideración y aprobación del Comité de Transparencia del INMEGEN.

Fecha de actualización	Motivo de la Actualización