DOCUMENTO DE SEGURIDAD

Instituto Nacional de Perinatología Isidro Espinosa de los Reyes

Montes Urales 800, Lomas Virreyes. Alcaldía Miguel Hidalgo, C.P. 11000. Ciudad de México.
Tel. (55) 5520.9900 · www.gob.mx/salud/inper

ÍNDICE

Montes Urales 800, Lomas Virreyes. Alcaldía Miguel Hidalgo, C.P. 11000. Ciudad de México.
Tel. (55) 5520.9900 · www.gob.mx/salud/inper

GLOSARIO

CPEUM	Constitución Política de los Estados Unidos Mexicanos
Lineamientos Generales	Lineamientos Generales de Protección de Datos para el Sector Público
LGPDPPSO	Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
INAI	Instituto Nacional de Transparencia Acceso a la Información Pública y Protección de Datos Personales
INPER	Instituto Nacional de Perinatología Isidro Espinosa de los Reyes.
LGTAIP	Ley General de Transparencia y Acceso a la Información Pública.

Montes Urales 800, Lomas Virreyes. Alcaldía Miguel Hidalgo, C.P. 11000. Ciudad de México.
Tel. (55) 5520.9900 · www.gob.mx/salud/inper

INTRODUCCIÓN

En atención a los artículos 1°, 2 fracción III, 5 fracción VII, 8 y 10 de la Ley de los Institutos Nacionales de Salud; 14, 15 de la Ley Federal de las Entidades Paraestatales y 1° del Estatuto Orgánico del Instituto Nacional de Perinatología Isidro Espinosa de los Reyes, se declara que el **INPER**, es un Organismo Descentralizado de la Administración Pública Federal, con personalidad jurídica y patrimonio propios, agrupado en el Sector Salud, que tiene por objeto principal, en el campo de la salud reproductiva y perinatal, la investigación científica, la formación y capacitación de recursos humanos calificados y la prestación de servicios de atención médica de alta especialidad, y cuyo ámbito de acción comprende todo el territorio nacional.

Asimismo, con la finalidad de garantizar la protección de datos personales en posesión de sujetos obligados, consagrados en los artículos 6o., Base A y 16, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos (CPEUM), el congreso General de los Estados Unidos Mexicanos ha expedido la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), la cual es de orden público y de observancia general en toda la República.

En esa tesitura, el Instituto Nacional de Transparencia Acceso a la Información Pública y Protección de Datos Personales (INA), como organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, con plena autonomía técnica, de gestión, capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, responsable de garantizar el cumplimiento del derecho de acceso a la información pública y a la protección de datos personales en posesión de los sujetos obligados, con fundamento en su artículo 6, apartado A, fracción VIII de la CPEUM y 89, fracciones XVII, XIX, XXVII Y XXVIII, 157 y quinto transitorio de la Ley General de Protección de Datos Personales, el Instituto cuenta con atribuciones para emitir disposiciones generales para el desarrollo del procedimiento de verificación; disposiciones administrativas de carácter

Montes Urales 800, Lomas Virreyes. Alcaldía Miguel Hidalgo, C.P. 11000. Ciudad de México.
Tel. (55) 5520.9900 · www.gob.mx/salud/inper

general para el cumplimiento de los principios, deberes, obligaciones, así como el ejercicio de los derechos de los titulares; lineamientos generales para el debido tratamiento de los datos personales, así como lineamientos para homologar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, ha emitido la normatividad denominada Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos generales).

En concordancia a la normatividad anterior, el presente documento de seguridad se elabora para dar cumplimiento con lo establecido en el artículo 35 de la LGPDPPSO y el INPER será el responsable del tratamiento de datos personales que recabe.

Montes Urales 800, Lomas Virreyes. Alcaldía Miguel Hidalgo, C.P. 11000. Ciudad de México.
Tel. (55) 5520.9900 · www.gob.mx/salud/inper

Inventario de datos personales y de los sistemas de tratamiento

Los numerales 33 fracciones I y III, y 35 fracción I de la LGPDPPSO, así como, numerales 58 y 59 de los Lineamientos Generales, establece la obligación de elaborar un inventario de datos personales y de los sistemas de tratamiento; que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión. El INPER, elaboró el siguiente inventario:

No.	Área	Nombre del Tratamiento	Inventario
1	Dirección Médica Departamento de Tecnologías de la Información.	Control de Citas	Control de Citas (Citas de Valoración)
2	Dirección de Administración y Finanzas. Departamento de Tecnologías de la Información.	Reclutamiento de Personal (Bolsa de Trabajo)	Recursos Humanos
3	Dirección de Educación en Ciencias de la Salud	Reclutamiento de Médicos Residentes y Curso de Especialización y Curso de Posgrado en alta especialidad (CPAEM)	Educación y Formación
4	Dirección Médica Departamento de Tecnologías de la Información	Sistema de Información y Gestión Institucional.	Consulta Externa (Atención Médica)
Total: 4			

Montes Urales 800, Lomas Virreyes. Alcaldía Miguel Hidalgo, C.P. 11000. Ciudad de México.
Tel. (55) 5520.9900 · www.gob.mx/salud/inper

El ciclo de vida de los datos personales, estará sujeto a la normativa regulada en materia de archivos, esto es por el Catálogo de disposición documental registro general y sistemático que establece los valores documentales, la vigencia documental, los plazos de conservación y la disposición documental, para el caso que corresponda. Información publicada en la fracción XLV del artículo 70 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), en la Plataforma Nacional de Transparencia (liga de consulta: https://consultapublicamx.plataformadetransparencia.org.mx/vut-web/?idSujetoObigadoParametro=206&idEntidadParametro=33&idSectorParametro=21)

Funciones y obligaciones de las personas que traten datos personales

Para dar cumplimiento al artículo 33 fracción II de la LGPDPPSO y 57 de los Lineamientos Generales, en la cual se establece que se debe definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales; se ha definido que el INPER cuenta con los roles en cada uno de los tratamientos y sus funciones como servidores públicos están ligados a la función del Manual de Organización Específico del INPER, el cual puede ser consultado en la siguiente liga: file:///D:/Users/transparencia.1.INPER/Downloads/50648_MOE-INPer-20161003Editable.pdf

Análisis de riesgos

Para dar cumplimiento al artículo 33 fracción IV de la LGPDPPSO y 60 de los Lineamientos Generales, en la cual se debe considerar las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, así como:

Montes Urales 800, Lomas Virreyes. Alcaldía Miguel Hidalgo, C.P. 11000. Ciudad de México.
Tel. (55) 5520.9900 · www.gob.mx/salud/inper

I. Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico;
II. El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida;
III. El valor y exposición de los activos involucrados en el tratamiento de los datos personales;
IV. Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida, y
V. Los factores previstos en el artículo 32 de la LGPDPSO.

Por lo anterior el INPER, realiza una valoración de activos en función de los tres principios fundamentales de seguridad de la información: confidencialidad, integridad y disponibilidad, de lo anterior se identifican las amenazas, vulnerabilidades y escenarios de vulneración.

Análisis de Brecha

Para dar cumplimiento al artículo 33 fracción V de la LGPDPPSO y 61 de los Lineamientos Generales, en la cual deberá considerar lo siguiente:

I. Las medidas de seguridad existentes y efectivas;
II. Las medidas de seguridad faltantes, y
III. La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.

Una vez que el INPER ha evaluado el riesgo se realiza el análisis de brecha, para tomar mejores decisiones, por lo cual, se realizará lo siguiente.

a) Investigar **qué controles o medidas de seguridad ya están funcionando en la Organización y si lo hacen de manera efectiva.** Esto requiere evaluar su eficacia frente al riesgo.
b) **Medir el nivel de madurez de las medidas de seguridad.** Que tan correctamente implementadas están en el sujeto obligado.
c) Las medidas faltantes (contar con una base de comparación).
d) Si existen nuevas medidas de seguridad que puedan reemplazar a uno o más controles implementados actualmente. (Toma de decisiones informada).

Montes Urales 800, Lomas Virreyes. Alcaldía Miguel Hidalgo, C.P. 11000. Ciudad de México.
Tel. (55) 5520.9900 · www.gob.mx/salud/inper

Plan de Trabajo

De conformidad con lo dispuesto en el artículo 33, fracción VI de la LGPDPPSO y 62 de los Lineamientos Generales, el responsable deberá elaborar un plan de trabajo que defina las 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.

Mecanismos de Monitoreo y Revisión de las Medidas de Seguridad

Con relación al artículo 33, fracción VII de la LGPDPPSO y 63 de los Lineamientos Generales, el responsable deberá evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, a fin de verificar el cumplimiento de los objetivos propuestos y, en su caso, implementar mejoras de manera continua.

Para cumplir con lo dispuesto en el párrafo anterior, el responsable deberá monitorear continuamente lo siguiente:

I. Los nuevos activos que se incluyan en la gestión de riesgos;
II. Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras;
III. Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;
IV. La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;
V. Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;

Montes Urales 800, Lomas Virreyes. Alcaldía Miguel Hidalgo, C.P. 11000. Ciudad de México.
Tel. (55) 5520.9900 · www.gob.mx/salud/inper

VI. El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y
VII. Los incidentes y vulneraciones de seguridad ocurridas.

Aunado a lo previsto en las fracciones anteriores, el responsable deberá contar con un programa de auditoría, interno y/o externo, para monitorear y revisar la eficacia y eficiencia del sistema de gestión, el cual estará sujeto al procedimiento de auditorías voluntarias por parte del INAI, cuando se solicite la práctica de auditoría voluntaria.

De lo anterior es posible identificar que el monitoreo y revisión de las medidas de seguridad tiene el objetivo de fortalecer, a través de un ciclo de mejora continua, la protección de los datos personales que resguarda este Instituto.

Mecanismos de Monitoreo

Para los tratamientos de datos personales, se consideran los siguientes tipos de monitoreo:

- **Revisión de cumplimiento de las políticas internas** de este sujeto obligado, relacionadas con el tratamiento de datos personales. Tiene el objetivo de asegurar que las personas servidoras públicas realicen los tratamientos de datos personales en concordancia con lo dispuesto en la LGPDPPSO, los Lineamientos Generales de Protección de Datos Personales para Sector Público, y demás normatividad que resulte aplicable.

  Para ello, cuando se identifica algún cambio en los instrumentos antes mencionados, se deberán realizar las siguientes actividades.
  a) Revisar y, en su caso, actualizar los procesos involucrados en el tratamiento de datos personales.
  b) Revisar y, en su caso, actualizar los avisos de privacidad, las funciones y obligaciones del personal y los inventarios de datos personales, según corresponda.
  c) 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.

Montes Urales 800, Lomas Virreyes. Alcaldía Miguel Hidalgo, C.P. 11000. Ciudad de México.
Tel. (55) 5520.9900 · www.gob.mx/salud/inper

d) Revisar y, en su caso, adecuar los sistemas de tratamiento para cumplir con los cambios normativos.

- **Revisión del riesgo**. Tiene el objetivo de identificar modificaciones a los riesgos identificados en los tratamientos de datos personales, para ello, se implementarán los siguientes monitoreos:
  a) Monitoreo del entorno físico. Para la detección continua de amenazas y vulnerabilidades en el entorno físico, se cuenta con: (i) personal de vigilancia en los accesos del edificio del Instituto, (ii) control de acceso del personal con credencial de servidor público o gafete de acceso, (iii) control de acceso a través de bitácoras para visitantes y personal adscrito a este sujeto obligado que olvidó su credencial, (iv) control de asistencia a través de huella digital, y (v) circuito cerrado de cámaras de vigilancia.
  b) Monitoreo del entorno electrónico. Para la detección continua de amenazas y vulnerabilidades, el Departamento de Tecnologías de la Información cuenta con herramientas automatizadas de monitoreo (activo y pasivo), así como con bitácoras de los sistemas informáticos.
  c) Actualización del plan de trabajo. Derivado del monitoreo del entorno físico o electrónico, se pueden realizar actualizaciones en el plan de trabajo en caso de que se identifiquen cambios en las amenazas, las vulnerabilidades o el impacto de los riesgos identificados. Estos cambios se pondrán a consideración del área que apoya en el análisis de riesgos, el Departamento de Tecnologías de la Información y la Unidad de Transparencia.
  d) Revisión de avances del plan de trabajo. A través de los mecanismos que determine el área que apoya en el análisis de riesgos, el Departamento de Tecnologías de la Información y la Unidad de Transparencia, se hará una revisión de los avances en el plan de trabajo, identificando las acciones, fechas compromiso y, en su caso, las causas por las cuales no se está cumpliendo el plan de trabajo, para hacer los ajustes correspondientes al mismo.

Montes Urales 800, Lomas Virreyes. Alcaldía Miguel Hidalgo, C.P. 11000. Ciudad de México.
Tel. (55) 5520.9900 · www.gob.mx/salud/inper

e) Actualización tecnológica. Cuando se integren nuevos equipos de cómputo, servidores, aplicaciones o tenga lugar una migración tecnológica, se realizará una actualización del análisis de riesgo, análisis de brecha y plan de trabajo.
f) Vulneraciones a la seguridad de los datos personales. En caso de identificar un incidente de seguridad que involucre datos personales, el área que apoya en el análisis de riesgos, Departamento de Tecnologías de la Información y la Unidad de Transparencia se coordinarán para decidir sobre las acciones pertinentes para mitigar dicho incidente.

Mecanismos de supervisión o revisión

Además del monitoreo continuo de las medidas de seguridad, se requiere realizar una supervisión periódica de las medidas de seguridad, a través de auditorías, las cuales pueden ser internas o externas, sujeta a la disponibilidad presupuestal, predominando en todo momento, a un procedimiento de auditorías voluntarias por parte del INAI, cuando se solicite la práctica de auditoría voluntaria.

Programa General de Capacitación

Con relación al artículo 30, fracción III de la LGPDPPSO, y 48 de los Lineamientos Generales, el responsable deberá establecer anualmente un programa de capacitación y actualización en materia de protección de datos personales dirigido a su personal y a encargados, el cual deberá ser aprobado, coordinado y supervisado por su Comité de Transparencia.

El programa de capacitación está a cargo de la Unidad de Transparencia, la cual deberá ser revisado y actualizado continuamente, que comprenda el ejercicio actual del que se trate y publicarlo en la sección de Protección de Datos Personales de la página del Instituto.

Montes Urales 800, Lomas Virreyes. Alcaldía Miguel Hidalgo, C.P. 11000. Ciudad de México.
Tel. (55) 5520.9900 · www.gob.mx/salud/inper