DOCUMENTO DE SEGURIDAD DEL INSTITUTO NACIONAL DE PERINATOLOGÍA ISIDRO ESPINOSA DE LOS REYES.

DOCUMENTO DE SEGURIDAD DEL INSTITUTO NACIONAL DE PERINATOLOGÍA "ISIDRO ESPINOSA DE LOS REYES"

El presente documento de seguridad se elabora para dar cumplimiento con lo establecido en el artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO).

Para efectos del presente documento, se entenderá como responsable en términos a los sujetos obligados a que se refiere el artículo 1 de la LGPDPPSO que deciden sobre el tratamiento de datos personales, el Instituto Nacional de Perinatología Isidro Espinosa de los Reyes en adelante el **INPer**, asimismo, para la implementación del documento de seguridad para cada área administrativa adscrita al INPer serán los responsables de recabar los datos personales y dar un tratamiento con la finalidad de apoyar con el objeto principal de este Instituto, 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 de conformidad con su artículo 1 del Estatuto Orgánico del INPer.

1. Políticas internas para la gestión y tratamiento de los datos personales

El INPer deberá:

Crear políticas internas para la gestión y tratamiento de los datos personales, 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.

En ese contexto, se definirá de acuerdo con las facultades estipuladas en el Estatuto Orgánico del INPer, así como, en sus Manuales de Procedimientos, con la finalidad materializar sus funciones encomendadas.

De lo anterior, también se recomienda tomar en consideración la implementación o actualización de los avisos de privacidad integral y simplificado.

2. Funciones y obligaciones del personal

El INPer deberá:

Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales.

Montes Urales 800, Lomas Virreyes. Miguel Hidalgo, Ciudad de México C.P. 11000
Teléfono 5520.9900 ext. 424, 528 · transparencia@inper.gob.mx

Se definirá de acuerdo con las facultades estipuladas en el Estatuto Orgánico del INPer, así como, en sus Manuales de Procedimientos y área de adscripción.

Documento de Seguridad: _____*Anotar el nombre del documento de seguridad específico*_____	
Objetivo:	
Número consecutivo:	**INPER-DS-CLAVE DE ÁREA-CONSECUTIVO**
Fecha de Aprobación ante el Comité de Transparencia:	

Responsable	
Nombre:	
Cargo:	
Funciones:	
Obligaciones:	

Usuarios	
Nombre:	
Cargo:	
Funciones:	
Obligaciones:	
Acuerdo de Confidencialidad.	Guardar confidencialidad respecto de los procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales , obligación que subsistirá aún después de finalizar sus relaciones con el mismo, y con el INPer.

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

El INPer deberá:

Elaborar un inventario de datos personales y de los sistemas de tratamiento

Se entenderá como tratamiento cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

Montes Urales 800, Lomas Virreyes. Miguel Hidalgo, Ciudad de México C.P. 11000
Teléfono 5520.9900 ext. 424, 528 · transparencia@inper.gob.mx

En ese contexto, se definirá si el tratamiento de datos personales obra en soportes físicos o electrónicos, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Inventario de Datos Personales			
Tipo de Datos	**Datos Personales**	**Soporte**	
		Físico	**Electrónico**
Datos Personales			
Datos Bancarios			
Datos Fiscales			
Datos Laborales			
Datos Sensibles*			

*Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;

3.1 Responsable y Encargado

En atención a los deberes a que se refiere la LGPDPPSO, el presente documento, es aplicable para todas las unidades administrativas del INPer que, en el ejercicio de sus atribuciones y funciones, administren bases de datos en sistemas de tratamiento de datos personales, ya sea que administren sistemas completos, o el tramo de información corresponda.

Además de las funciones y obligaciones de los servidores públicos involucrados, establecidas de manera específica en el análisis de cada uno de los Sistemas de manera general, deberá de observarse lo siguiente:

- Realizar el tratamiento de los datos personales conforme a las instrucciones del responsable.
- Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable.
- Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables.
- Informar al responsable cuando ocurra una vulneración a los datos personales que trata por sus instrucciones.

Montes Urales 800, Lomas Virreyes. Miguel Hidalgo, Ciudad de México C.P. 11000
Teléfono 5520.9900 ext. 424, 528 · transparencia@inper.gob.mx

- Guardar confidencialidad respecto de los datos personales tratados.
- Suprimir o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales.
- Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.

3.2 Transferencias y Remisiones

Se entenderá como transferencia, toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado, y como remisión, toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano.

Las remisiones nacionales e internacionales de datos personales que se realicen entre responsable y encargado no requerirán ser informadas al titular, ni contar con su consentimiento.

Transferencia			
Marcar con una X, si es Nacional o Internacional la Transferencia			
Nacional		Internacional	
Nombre del Responsable:			
Cargo:			
Teléfonos Institucionales y Extensiones:			
Correo electrónico institucional:			
Nombre a quién le realizan la transferencia:			
Cargo:			
Teléfonos y Extensiones:			
Correo electrónico:			
Notificación al titular de los datos personales:			
Medio de Notificación:			

Montes Urales 800, Lomas Virreyes. Miguel Hidalgo, Ciudad de México C.P. 11000
Teléfono 5520.9900 ext. 424, 528 · transparencia@inper.gob.mx

4. Análisis de riesgo de los datos personales

El INPer deberá:

Realizar un análisis de riesgo de los datos personales, considerando 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, entre otros.

4.1 Sistema de Gestión (Medidas de Seguridad Administrativas, Físicas y Técnicas)

Las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión.

Se entenderá por sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales.

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.

Medidas de Seguridad		
Tipo de Medidas de Seguridad	Características	Seguridad
Administrativas	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.	• Llevar a cabo la revisión y protección de datos personales

Montes Urales 800, Lomas Virreyes. Miguel Hidalgo, Ciudad de México C.P. 11000
Teléfono 5520.9900 ext. 424, 528 · transparencia@inper.gob.mx

Físicas	Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.	• Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información. • Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información. • Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización. • Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad;
Técnicas	Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento	• Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados. • Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones. • Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware. • Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Montes Urales 800, Lomas Virreyes. Miguel Hidalgo, Ciudad de México C.P. 11000
Teléfono 5520.9900 ext. 424, 528 · transparencia@inper.gob.mx

4.2 Actualización del Documento de Seguridad

El responsable deberá actualizar el documento de seguridad cuando ocurran los siguientes eventos:

- Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo.
- Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión.
- Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida.
- Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

En caso de que ocurra una vulneración a la seguridad, el responsable deberá analizar las causas por las cuales se presentó e implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales si fuese el caso a efecto de evitar que la vulneración se repita.

Además de las que señalen las leyes respectivas y la normatividad aplicable, se considerarán como vulneraciones de seguridad, en cualquier fase del tratamiento de datos, al menos, las siguientes:

- La pérdida o destrucción no autorizada.
- El robo, extravío o copia no autorizada.
- El uso, acceso o tratamiento no autorizado.
- El daño, la alteración o modificación no autorizada.

El responsable deberá llevar una bitácora de las vulneraciones a la seguridad en la que se describa ésta, la fecha en la que ocurrió, el motivo de ésta y las acciones correctivas implementadas de forma inmediata y definitiva.

El responsable deberá informar sin dilación alguna al titular, y según corresponda, al Instituto y a los Organismos garantes de las Entidades Federativas, las vulneraciones que afecten de forma significativa los derechos patrimoniales o morales, en cuanto se confirme que ocurrió la vulneración y que el responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, a fin de que los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos.

Montes Urales 800, Lomas Virreyes. Miguel Hidalgo, Ciudad de México C.P. 11000
Teléfono 5520.9900 ext. 424, 528 · transparencia@inper.gob.mx

El responsable deberá informar al titular al menos lo siguiente:

- La naturaleza del incidente.
- Los datos personales comprometidos.
- Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses.
- Las acciones correctivas realizadas de forma inmediata.
- Los medios donde puede obtener más información al respecto.

El responsable deberá establecer controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales, guarden confidencialidad respecto de éstos, obligación que subsistirá aún después de finalizar sus relaciones con el mismo.

Lo anterior, sin menoscabo de lo establecido en las disposiciones de acceso a la información pública

Bitácora	
Nombre del Documento de Seguridad:	
Datos del Responsable	
Nombre:	
Cargo:	
Funciones:	
Obligaciones:	
Indicar si es una Actualización al Documento de Seguridad o es una Vulneración a la Seguridad del Tratamiento de Datos Personales.	
Naturaleza del incidente	
Datos personales comprometidos	
Recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses	
Acciones correctivas realizadas de forma inmediata y medios donde puede obtener más información al respecto.	
Notificación al Titular de los Datos Personales y medio de notificación.	
Plan de Trabajo:	Implementar las acciones preventivas y correctivas.

Montes Urales 800, Lomas Virreyes. Miguel Hidalgo, Ciudad de México C.P. 11000
Teléfono 5520.9900 ext. 424, 528 · transparencia@inper.gob.mx

4.3 Operación o modificación a políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología

Cuando el responsable pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que a su juicio y de conformidad con esta Ley impliquen el tratamiento intensivo o relevante de datos personales, deberá realizar una Evaluación de impacto en la protección de datos personales, y presentarla ante el Instituto o los Organismos garantes, según corresponda, los cuales podrán emitir recomendaciones no vinculantes especializadas en la materia de protección de datos personales.

El contenido de la evaluación de impacto a la protección de datos personales deberá determinarse por el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.

Se considerará que se está en presencia de un tratamiento intensivo o relevante de datos personales cuando:

- Existan riesgos inherentes a los datos personales a tratar.
- Se traten datos personales sensibles.
- Se efectúen o pretendan efectuar transferencias de datos personales.

El Instituto y los Organismos garantes, según corresponda, deberán emitir, de ser el caso, recomendaciones no vinculantes sobre la Evaluación de impacto en la protección de datos personales presentado por el responsable.

El plazo para la emisión de las recomendaciones a que se refiere el párrafo anterior será dentro de los treinta días siguientes contados a partir del día siguiente a la presentación de la evaluación.

Cuando a juicio del sujeto obligado se puedan comprometer los efectos que se pretenden lograr con la posible puesta en operación o modificación de políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales o se trate de situaciones de emergencia o urgencia, no será necesario realizar la Evaluación de impacto en la protección de datos personales.

5. Análisis de brecha

Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable.

Montes Urales 800, Lomas Virreyes. Miguel Hidalgo, Ciudad de México C.P. 11000
Teléfono 5520.9900 ext. 424, 528 · transparencia@inper.gob.mx

6. Plan de trabajo

Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales.

Plan de Trabajo	
Nombre del Documento de Seguridad:	
Datos del responsable	
Nombre:	
Cargo:	
Funciones:	
Obligaciones:	
Acciones Preventivas:	
Acciones Correctivas:	
Medidas de seguridad implementadas:	
Actividades: Reunión con las áreas involucradas y/o responsables Capacitación sobre análisis de riesgos y confidencialidad Análisis de riesgos Proyecto de Sistema de seguridad de datos personales Revisión y modificación al documento de seguridad y avisos de privacidad Monitoreo y análisis de brecha	

Montes Urales 800, Lomas Virreyes. Miguel Hidalgo, Ciudad de México C.P. 11000
Teléfono 5520.9900 ext. 424, 528 · transparencia@inper.gob.mx

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

Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales.

8. Programa general de capacitación

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

Montes Urales 800, Lomas Virreyes. Miguel Hidalgo, Ciudad de México C.P. 11000
Teléfono 5520.9900 ext. 424, 528 · transparencia@inper.gob.mx