DOCUMENTO DE SEGURIDAD

Instituto Nacional de Enfermedades Respiratorias
Ismael Cosío Villegas

Septiembre 2024

ÍNDICE

Contenido	**Pág.**
Glosario	2
Introducción	3
I. Inventario de datos personales y de los sistemas de tratamiento	4
II. Funciones y obligaciones de las personas que traten datos personales	9
III. Análisis de riesgos	9
IV. Análisis de brecha	10
V. Plan de Trabajo	10
VI. Mecanismos de monitoreo y revisión de las medidas de seguridad	11
VII. Programa General de Capacitación	14
VIII. Actualización del documento de seguridad	15

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
INER	Instituto Nacional de Enfermedades Respiratorias Ismael Cosío Villegas
LGTAIP	Ley General de Transparencia y Acceso a la Información Pública.
INAI	Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales

INTRODUCCIÓN

En atención a los artículos 1°, 2 fracción III, 5 fracción IV, 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 Enfermedades Respiratorias Ismael Cosío Villegas, se declara que el **INER**, 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 padecimientos del aparato respiratorio, la investigación científica, la formación y capacitación de recursos humanos calificados y la prestación de servicios de atención médica de alta especialidad, cuyo ámbito de competencia es todo el territorio nacional.

De esta manera, 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. Asimismo, los Lineamientos Generales de Protección de Datos Personales para el Sector Público, indican que los sujetos obligados, es decir, el responsable; deberá observar ocho principios y dos deberes en el tratamiento de datos personales. Dichos principios son: licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, en tanto que los deberes son: confidencialidad y seguridad.

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 INER será el responsable del tratamiento de datos personales que recabe.

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

De acuerdo con lo previsto en los artículos 33 fracciones I y III, y 35 fracción I de la LGPDPPSO, así como, los 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 INER, elaboró el siguiente inventario:

No.	Áreas	No. de procesos	Nombre del tratamiento
1	Departamento de Asuntos Jurídicos	5	1. Dictaminación de actas circunstanciadas 2. Elaboración de contratos y convenios 3. Asuntos contenciosos 4. Atención de quejas administrativas 5. Certificación de documentos
2	Unidad de Transparencia	4	1. Atención de solicitudes de derechos ARCO 2. Atención de solicitudes de información pública 3. Atención a recursos de revisión 4. Atención a peticiones ciudadanas
3	Departamento de Calidad	1	1. Sistema Unificado de Gestión y atención a los usuarios de servicios de salud
4	Departamento de Trabajo Social	2	1. Procedimiento para la atención, registro e identificación de pacientes en pre consulta y Consulta Externa 2. Procedimiento para la atención, registro e identificación de pacientes en los servicios de Admisión y Urgencias
5	Servicio de Banco de Sangre	1	1. Donación de sangre y plaquetas en el Banco de Sangre
6	Servicio de Medicina Nuclear	3	1. Pacientes externos (referidos) 2. Pacientes de consulta externa 3. Pacientes hospitalizados

7	Servicio de Electrocardiograma	3	1. Atención de pacientes en consulta externa 2. Procedimientos para la realización de estudio de gabinete no invasivos 3. Procedimientos para la realización de estudios y tratamientos invasivos
8	Departamento de Patología	4	1. Realización de estudios citológicos 2. Realización de estudios histopatológicos de biopsias y piezas quirúrgicas (órganos) 3. Estudios post-mortem
9	Departamento de Radiología	1	1. Realización de Estudios de Rayos X
10	Servicio de Rehabilitación Pulmonar	3	1. Consulta de primera vez al Servicio de Rehabilitación Pulmonar 2. Realización de prueba de esfuerzo 3. Estratificación de riesgo respiratorio
11	Departamento de Unidad de Epidemiología Hospitalaria e Infectología	2	1. Vigilancia epidemiológica 2. Generación de estadísticas de morbilidad y mortalidad
12	Laboratorio Clínico	6	1. Procedimiento del área de toma de muestra sanguínea 2. Procedimiento de recepción de muestras 3. Procedimiento para el transporte de muestras 4. Procedimiento del área de Química de rutina 5. Procedimiento del funcionamiento de pruebas especiales rutina 6. Procedimiento del área de urgencias
13	Coordinación de Registros Médicos y Admisión Hospitalaria	7	1. Apertura de expediente clínico 2. Solicitud de expediente clínico para consulta externa 3. Solicitud de expediente clínico para protocolos de investigación 4. Solicitud de expediente clínico para presentación de sesiones médicas 5. Recepción de expedientes clínicos de pacientes egresados de piso 6. Depuración de expedientes clínicos activos 7. Depuración de expedientes clínicos inactivos

14	Servicio de Infectología y Microbiología Clínica	3	1. Atención de pacientes de consulta externa y hospitalización 2. Procedimiento para toma de muestras microbiológicas 3. Recepción, revisión y criterios de
15	Consulta Externa	3	1. Recepción de pacientes de nuevo ingreso 2. Referencia de pacientes a otros institutos 3. Atención a pacientes subsecuentes
16	Unidad de Urgencias	5	1. Atención médica 2. Hospitalización o Cirugía 3. Procedimiento para referencia y contra Referencia de pacientes que requieren atención médica en otra institución 4. Egreso del paciente de la Unidad de Urgencias 5. Egreso por defunción
17	Hospitalización	7	1. Identificación del paciente para brindar diagnóstico y tratamiento 2. Manejo y Tratamiento médico 3. Elaboración de notas médicas 4. Solicitud de estudios de gabinete 5. Elaboración de consentimiento informado 6. Elaboración de indicaciones médicas
18	Departamento de Áreas Críticas	6	1. Elaboración de notas médicas 2. Solicitud de estudios de gabinete 3. Elaboración de consentimiento informado 4. Notas médicas 5. Elaboración de indicaciones médicas 6. Solicitud de transfusiones
19	Dirección de investigación	1	1. Desarrollo de Proyectos de investigación

20	Dirección de Enseñanza	5	1. Selección de aspirantes a los Programas de Posgrado 2. Aceptación de alumnos de servicio social y estancias de pregrado 3. Aceptación de Rotaciones Clínicas (Médicos Externos) 4. Asistencia a Cursos de Educación Médica Continua (presencial y/o virtual) 5. Asistencia a Cursos a distancia
21	Departamento de Enfermería	6	1. Inducción al puesto de enfermería y al servicio asignado 2. Educación y capacitación continua en servicio 3. Capacitación en tecnología 4. Prácticas clínicas 5. Educación para la salud 6. Evaluación de estándares de calidad del cuidado
22	Escuela de Enfermería	5	1. Proceso de selección para ingreso a la Escuela 2. Ingreso a la plataforma DGIRE-UNAM 3. Expediente UNAM 4. Actualización de procesos académicos del alumno 5. Proceso de titulación
23	Subdirección de Planeación	2	1. Elaboración de informes oficiales para contribuir al análisis del desempeño institucional 2. Intercambio de información para cumplir los objetivos institucionales
24	Subdirección de Administración y Desarrollo de Personal	4	1. Reclutamiento y selección de personal 2. Inscripción de médicos residentes al Instituto Nacional de Enfermedades Respiratorias 3. Integración de expedientes y clasificación en el archivo de la Subdirección de Administración y Desarrollo de Personal 4. Resguardo de expediente laboral

2024 AÑO DE Felipe Carrillo PUERTO BENEMÉRITO DEL PROLETARIADO, REVOLUCIONARIO Y DEFENSOR DEL MAYAB

25	Subdirección de Recursos Materiales y Servicios Generales	3	1. Coordinar y supervisar el cumplimiento de los planes y programas de trabajo de las áreas a su cargo o inmediatos inferiores. 2. Supervisar las adquisiciones y vigilar el pago a proveedores 3. Recepción, almacenamiento, conservación y suministro de los bienes de consumo
26	Departamento de Informática	3	1. Generación de correos institucionales 2. Generación de cuentas de usuarios en sistemas internos 3. Proporcionar servicios informáticos de implementación y soporte a través de soluciones tecnológicas
27	Farmacia Hospitalaria	3	1. Entrega de insumos médicos a las áreas solicitantes 2.Dispensación de medicamentos controlados, estupefacientes y psicotrópicos
28	Subdirección de Recursos Financieros	2	1. Operación de sistemas contables 2. Elaboración de facturas 3. Registro e información de los recursos externos para fines del
29	Seguridad y Servicios	2	1. Video vigilancia de instalaciones 2. Acceso peatonal en puertas

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

De acuerdo con lo previsto en el 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 INER 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 INER, el cual puede ser consultado en la siguiente liga: https://www.gob.mx/cms/uploads/attachment/file/670143/MO_INER_2016-2.pdf

III. 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:

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.

De acuerdo a lo anteriormente el INER, 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 posibles amenazas y vulnerabilidades.

IV. Análisis de Brecha

Para dar cumplimiento al artículo 33 fracción V de la LGPDPPSO y 61 de los Lineamientos Generales, en la cual el responsable 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, se haya evaluado el riesgo se realizará el análisis de brecha, para tomar mejores decisiones, por lo cual, se efectuará lo siguiente:

a) Investigar qué medidas de seguridad están funcionando y si lo hacen de manera efectiva. Esto requiere evaluar su eficacia frente al riesgo.
b) Nivel de las medidas de seguridad y si están implementadas correctamente en el sujeto obligado.
c) Si existen nuevas medidas de seguridad que puedan reemplazar a uno o más controles implementados actualmente. (Toma de decisiones informada).

V. 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.

VI. Mecanismos de Monitoreo y Revisión de las Medidas de Seguridad

En cumplimiento 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;
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.

Por lo anterior, es posible identificar que el monitoreo y revisión de las medidas de seguridad tiene el objetivo de fortalecer, la protección de los datos personales que resguarda el Instituto.

Mecanismos de Monitoreo

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

- **Revisión de cumplimiento de las políticas internas del INER, 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.
  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 fotografía con lector de la credencial, y (v) circuito cerrado de cámaras de vigilancia.

b. Monitoreo del entorno electrónico. Para la detección continua de amenazas y vulnerabilidades, el Departamento de Informática 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 Informática y el Comité 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 Informática y el Comité 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.

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 Informática y el Comité 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, mismas que 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.

VII. Programa General de Capacitación

Con relación a los artículos 30, fracción III y 33 fracción VIII de la LGPDPPSO, así como el artículo 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.

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.

El programa de capacitación está a cargo de la Unidad de Transparencia, el cual deberá ser revisado y actualizado continuamente, 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 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.

VIII. 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.