# Documento de Seguridad del Instituto Nacional de Pediatría.

## Comité de Transparencia.

SALUD
SECRETARÍA DE SALUD

Instituto Nacional de Pediatría
INP

**Trabajando por la Salud de Nuestra Niñez Mexicana.**

**Doc.7_Versión01_2024.**

# Contenido.

# I. Marco Normativo.

El presente documento tiene como base las disposiciones contenidas en los siguientes ordenamientos:

- Constitución Política de los Estados Unidos Mexicanos;
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;
- Ley General de Transparencia y Acceso a la Información Pública;
- Ley Federal de Transparencia y Acceso a la Información Pública;
- Lineamientos Generales de Protección de Datos Personales para el Sector Público;
- Lineamientos que establecen los Parámetros, Modalidades y Procedimientos para la Portabilidad de Datos Personales;
- Estatuto Orgánico del Instituto Nacional de Pediatría.
- Acuerdo mediante el cual el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, aprueba el Padrón de sujetos obligados del ámbito federal, en términos de la Ley General de Transparencia y Acceso a la Información Pública
- Acuerdo mediante el cual se aprueba que el Padrón de sujetos obligados del ámbito federal, en términos de la Ley General de Transparencia y Acceso a la Información Pública y sus respectivas actualizaciones llevadas a cabo por la Secretaría de Acceso a la Información, se utilice como referencia directa del catálogo de sujetos obligados en el ámbito federal para efectos de lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Manuales Administrativos de Aplicación General
- Normas internas Administrativas
- Normas Internas Sustantivas

# II. Términos y Definiciones.

**Aceptar el riesgo:** Decisión informada para coexistir con un nivel de riesgo.

**Activo:** En términos generales, un activo es cualquier elemento que representa un valor para la organización. Según la Real Academia Española, «valor» se define como: a) grado de utilidad o aptitud de las cosas para satisfacer las necesidades o proporcionar bienestar o deleite, y b) cualidad de las cosas, en virtud de la cual se da por poseerlas cierta suma de dinero o equivalente

**Amenaza:** Circunstancia o evento con la capacidad de causar daño a una organización.

**Análisis de riesgos:** Permite identificar los peligros y evaluar el nivel de riesgo hacia los datos personales. Las metodologías de análisis de riesgo establecen un proceso sistemático que consiste en crear escenarios de riesgo, identificando y correlacionando todos los elementos que intervienen en él: activo (que en el presente contexto consiste en los datos personales), amenazas, vulnerabilidades, controles existentes e impactos o consecuencias. Una vez creados los escenarios de riesgo, se procede a evaluar cualitativa o cuantitativamente el riesgo mediante el establecimiento de parámetros como la probabilidad de ocurrencia y el nivel de impacto o de beneficio para el atacante.

**Análisis de brecha:** Es planteado como la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.

**Áreas:** Instancias de los sujetos obligados previstas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes, que cuentan o puedan contar, dar tratamiento y ser responsables y encargadas de los datos personales.

**Archivo electrónico:** Información generada, almacenada o transmitida a través de medios electrónicos, ópticos o por cualquier otra tecnología, lo cual consiste en la propia definición de mensaje de datos

**Área productora:** Unidad administrativa del INP a la que, atendiendo al nivel jerárquico establecido en el organigrama vigente, desde el nivel de dirección hasta jefatura de departamento, se le asigna una clave por el Área Coordinadora de Archivos, recibe y produce documentos de archivo en el ejercicio de sus facultades, funciones o competencias, mismos que están bajo su responsabilidad, independientemente del soporte, espacio o lugar en que los resguarden.

**Aviso de privacidad:** Documento a disposición del titular de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de éstos.

**Autenticación:** Es aquella característica de un documento que permite identificar y vincular a las personas que lo crearon y/o que han aceptado o expresado su consentimiento para obligarse en términos de su contenido, sin que estas puedan repudiar su consentimiento o voluntad

**Bases de datos:** Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

**Borrado seguro:** Procedimiento para la eliminación en un dispositivo o medio de almacenamiento, conocido o por conocer, que impide la recuperación de los datos personales.

**Bloqueo:** La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda;

**Ciclo vital del documento:** Las tres fases por las que atraviesan los documentos de archivo, sea cual sea su soporte, desde su recepción o generación hasta su conservación permanente o baja documental, a saber: archivo de trámite, archivo de concentración y archivo histórico.

**Comité de Transparencia:** Instancia a la que hace referencia el artículo 43 de la Ley General de Transparencia y Acceso a la Información Pública.

**Compartir el riesgo:** Proceso donde se involucra a terceros para mitigar la pérdida generada por un riesgo en particular, sin que el dueño del activo afectado reduzca su responsabilidad.

**Comunicar el riesgo**: Compartir o intercambiar información acerca del riesgo; esto entre la alta dirección, custodios y demás involucrados

**Cómputo en la nube:** Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente;

**Confidencialidad:** Propiedad de la información para no estar a disposición o ser revelada a personas, entidades o procesos no autorizados.

**Consentimiento:** Manifestación de la voluntad, libre, específica, inequívoca e informada del titular a través de la cual acepta y autoriza el tratamiento de los datos personales que le conciernen

**Consejo Nacional:** Consejo Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales a que se refiere el artículo 32 de la Ley General de Transparencia y Acceso a la Información Pública.

**Control de seguridad en la red:** Configuración de equipo activo de telecomunicaciones y software para proteger la transmisión de datos personales

**Consentimiento**: Manifestación de la voluntad libre, específica e informada del titular de los datos mediante la cual se efectúa el tratamiento de los mismos;

**Custodios:** Aquellas personas servidoras públicas con responsabilidad funcional sobre los activos: responsables del departamento de datos, administradores de sistemas o responsables de un proceso o proyecto específico, entre otros.

**Datos personales:** Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

**Datos personales sensibles:** Los que se refieran a la esfera más íntima de la persona titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De modo enunciativo mas no limitativo, 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.

**Derechos ARCO:** Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.

**Disociación:** El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación de este.

**Disponibilidad:** Propiedad de un activo para ser accesible y utilizable cuando lo requieran personas, entidades o procesos autorizados.

**Divulgación:** publicar, extender y/o poner al alcance del público algo

**Documento de seguridad:** Instrumento que describe y da 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;

**Encargado:** Persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o juntamente con otras trate datos personales en nombre y por cuenta del responsable.

**Evaluación de impacto en la protección de datos personales:** Documento mediante el cual los sujetos obligados que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, valoran los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares, así como los deberes de los responsables y encargados, previstos en la normativa aplicable;

**Evitar el riesgo:** Acción para retirarse de una situación de riesgo o decisión para no involucrarse en ella.

**Fuentes de acceso público:** Aquellas bases de datos, sistemas o archivos que por disposición de ley puedan ser consultadas públicamente cuando no exista impedimento por una norma limitativa y sin más exigencia que, en su caso, el pago de una contraprestación, tarifa o contribución. No se considerará fuente de acceso público cuando la información contenida en la misma sea obtenida o tenga una procedencia ilícita, conforme a las disposiciones establecidas por la presente Ley y demás normativa aplicable;

**Identificar el riesgo:** Proceso para encontrar, enlistar y describir los elementos del riesgo.

**Impacto:** Una medida del grado de daño a los activos o cambio adverso en el nivel de objetivos alcanzados por una organización.

**Incidente:** Escenario donde una amenaza explota una vulnerabilidad o conjunto de vulnerabilidades.

**Integridad:** La propiedad de salvaguardar la exactitud y completitud de los activos

**Instituto:** Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, el cual es el organismo garante de la Federación en materia de protección de datos personales en posesión de los sujetos obligados;

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

**Medidas de 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;

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

De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

**a)** Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;

**b)** Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;

**c)** Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y

**d)** Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad;

**Medidas de seguridad 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.

De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

**a)** Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;

**b)** Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;

**c)** Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y

**d)** Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales;

**Organismo garante:** Aquel con autonomía constitucional especializado en materia de acceso a la información y protección de datos personales, en términos de los artículos 6o. y 116, fracción VIII de la Constitución Política de los Estados Unidos Mexicanos;

**Plataforma Nacional:** La Plataforma Nacional de Transparencia a que hace referencia el artículo 49 de la Ley General de Transparencia y Acceso a la Información Pública;

**Principio del menor privilegio:** Otorgamiento de los permisos necesarios y suficientes a un usuario autorizado para acceder a un sistema de información para el desempeño de sus actividades.

**Privacidad:** La privacidad se puede entender como el ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión

**Red de datos:** Conjunto de componentes electrónicos activos y medios de comunicación conocidos o por conocer tales como fibra óptica, enlaces inalámbricos, cable, entre otros, que permiten el intercambio de paquetes de datos entre dispositivos electrónicos para el procesamiento de información

**Reducir el riesgo:** Acciones tomadas para disminuir la probabilidad, las consecuencias negativas, o ambas, asociadas al riesgo.

**Remisión:** Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano; XXVIII.

**Responsable:** Los sujetos obligados a que se refiere el artículo 1 de la presente Ley que deciden sobre el tratamiento de datos personales;

**Retención del riesgo:** Aceptación de la pérdida generada por un riesgo en particular. Esta acción implica monitoreo constante del riesgo retenido.

**Riesgo:** Combinación de la probabilidad de un evento y su consecuencia desfavorable.

**Riesgo de seguridad:** Combinación de la posibilidad de que se materialice una amenaza y sus consecuencias negativas. Riesgo inherente: Riesgo intrínseco al activo, sin considerar las medidas de seguridad implementadas. Riesgo residual: El riesgo remanente después de tratar el riesgo.

**Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información, así como otras propiedades delimitadas por la normatividad aplicable.

**Servicios de nube privada:** Modelo de servicio de tecnología de información proporcionados bajo demanda al INP, en infraestructura propiedad el INP y que incluye cómputo, almacenamiento, plataforma, seguridad y respaldos.

**Servicios de nube pública:** Modelo de servicio de tecnología de información adquirida bajo demanda a terceros, operada en infraestructura ajena al INP

**Supresión:** La baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable;

**Sistema de Gestión de Seguridad de Datos Personales (SGSDP):** Sistema de gestión general para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales en función del riesgo de los activos y de los principios básicos de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad previstos en la Ley General, los Lineamientos Generales, normatividad secundaria y cualquier otro principio que la buena práctica internacional estipule en la materia.

**Sistemas para el tratamiento:** Conjunto de elementos mutuamente relacionados o que interactúan para realizar la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales, en medios físicos o electrónicos

**Soporte:** Medio, ya sea electrónico o físico, en el que se registra y guarda información, como lo es: el papel, así como los audiovisuales, fotográficos, fílmicos, digitales, electrónicos, sonoros y visuales, entre otros, y los que produzca el avance de la tecnología.

**Soportes electrónicos:** Son los medios de almacenamiento accesibles sólo a través del uso de algún dispositivo electrónico conocido o por conocer, que procese su contenido para examinar, modificar o almacenar los datos; tales como cintas magnéticas de audio, vídeo y datos, fichas de microfilm, discos ópticos (CDs, DVDs y Blue-rays), discos magneto ópticos, discos magnéticos (flexibles y duros) y demás medios para almacenamiento masivo no volátil.

**Soportes físicos:** Son los medios de almacenamiento accesibles de forma directa y sin intervención de algún dispositivo para examinar, modificar o almacenar los datos; tales como documentos, oficios, formularios impresos, escritos autógrafos, documentos de máquina de escribir, fotografías, placas radiológicas, carpetas, expedientes, entre otros;

**Sujeto obligado:** Son sujetos obligados por la Ley General. En el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.

**Titular:** Persona física a quien corresponden los datos personales.

**Tratamiento:** Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionados con:

**a) Obtener:** Recabar datos personales o documentos que contienen datos personales.

**b) Almacenar:** Guardar datos personales, mismos que pueden ser almacenados en documentos físicos, archivos digitales, sistemas informáticos u otros.

c) **Registrar:** Examinar datos personales en documentos físicos, archivos digitales, sistemas informáticos u otros.

d) **Conservar:** Resguardar y cuidar la permanencia e integridad de los datos personales en documentos físicos, archivos digitales, sistemas informáticos u otros.

e) **Poseer:** Tener, guardar o custodiar datos personales.

f) **Utilizar:** Servirse emplear los datos personales para los fines y facultades otorgados en el INP

g) **Organizar:** Estructurar el de orden datos personales para un fin determinado.

h) **Acceder:** Disponibilidad de los datos personales en documentos físicos, archivos digitales, sistemas informáticos u otros, para fines específicos.

i) **Manejar:** Emplear o tratar datos personales en documentos físicos, archivos digitales, sistemas informáticos u otros.

j) **Aprovechar:** Utilizar datos personales para un fin legitimo definido por la normatividad universitaria

k) **Elaborar:** Idear, o crear algún contenido a partir de documentos físicos, archivos digitales, sistemas informáticos u otros.

l) **Transferir:** Comunicar datos personales, dentro o fuera del territorio mexicano a una personal (moral o física) distinta del titular

m) **Comunicar:** Informar datos personales o algún elemento que contenga datos personales, al interior de las entidades o dependencias

n) **Difundir:** Propagar o divulgar datos personales.

o) **Divulgar:** Propagar o divulgar datos personales públicamente.

p) **Remitir:** Enviar datos personales a determinada persona de otro lugar.

q) **Disponer:** Determinar lo que ha de hacerse con los datos personales.

r) **Bloquear:** Impedir el uso de los datos personales.

s) **Cancelar:** Borrar o eliminar de forma permanente los datos personales

**Transferencia:** Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, responsable o encargado.

**Tratar el riesgo:** Procesos que se realizan para modificar el nivel de riesgo. Unidad de Transparencia: Instancia a la que hace referencia el artículo 45 de la Ley General de Transparencia y Acceso a la Información Pública.

**Valorar el riesgo:** Proceso para asignar valores a la probabilidad y consecuencias del riesgo.

**Vulnerabilidad:** Falta o debilidad de seguridad en un activo o grupo de activos que puede ser explotada por una o más amenazas.

# III. Introducción.

El derecho humano a la protección de datos personales se encuentra contemplado en los artículos 6o., Base A y 16, segundo párrafo de la Constitución Política de los Estados Unidos Mexicanos; asimismo, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Ley General), publicada en el Diario Oficial de la Federación el 26 de enero de 2017, tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados.

El artículo primero de la Ley General, indica que son sujetos obligados en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.

En virtud de lo anterior, el Instituto Nacional de Pediatría (INP), al ser un organismo público descentralizado de la Administración Pública Federal, que tiene por objeto principal garantiza el derecho de protección a la salud a los niñas, niños adolescente, la investigación científica, la formación y capacitación de recursos humanos calificados y la prestación de servicios de atención médica de alta especialidad; es un sujeto obligado de la Ley General, y debe dar cumplimiento a dicho ordenamiento jurídico respecto del tratamiento de datos personales que realice en el ejercicio de sus funciones.

La Ley General y los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos), 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.

Aunado a lo anterior, la Constitución reconoce a los titulares de los datos personales el ejercicio de sus derechos ARCO (acceso, rectificación, cancelación y oposición), cuyos procedimientos se encuentran previstos en la Ley General y Lineamientos; asimismo, la Ley General reconoce el derecho de portabilidad.

Para el cumplimiento de dichos principios, deberes y derechos, el Instituto Nacional de Pediatría deberá observar las obligaciones previstas en los instrumentos normativos antes señalados, de tal forma que pueda garantizar la confidencialidad, integridad y disponibilidad de los datos personales a los que da tratamiento.

En cuanto al deber de seguridad, el artículo 31 de la Ley General indica que el responsable del tratamiento de datos personales, deberá establecer y mantener las 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.

En relación con lo anterior, el artículo 33 señala que, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:

I. 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;

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

III. Elaborar un inventario de datos personales y de los sistemas de tratamiento;

IV. 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;

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

VI. 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;

VII. 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, y

VIII. 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.

Asimismo, en el artículo 35 de la Ley General se establece la obligación de elaborar un documento de seguridad, que de acuerdo con lo dispuesto en el artículo 3, fracción XIV, se define como:

Instrumento que describe y da 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.

Mismo que de conformidad con lo establecido en el artículo 35 de la Ley General, deberá contener al menos lo siguiente:

I. El inventario de datos personales y de los sistemas de tratamiento;

II. Las funciones y obligaciones de las personas que traten datos personales;

III. El análisis de riesgos;

IV. El análisis de brecha;

V. El plan de trabajo;

VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y

VII. El programa general de capacitación.

En virtud de lo anterior, el Instituto Nacional de Pediatría elabora el presente documento de seguridad, atendiendo los requisitos previstos en el artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

# IV. Contexto del Instituto Nacional de Pediatría.

El Instituto Nacional de Pediatría es un organismo público descentralizado dependiente de la Comisión Coordinadora de los Institutos Nacionales de Salud y Hospitales de Alta Especialidad de la Secretaría de Salud, con 50 años de experiencia operativa.

Que es un organismo público descentralizado de la Administración Pública Federal con personalidad jurídica y patrimonio propios, que rigen su organización y funcionamiento según lo dispuesto por la Ley de los Institutos Nacionales de Salud publicada en el Diario Oficial de la Federación el veintiséis de mayo del año dos mil; de conformidad con lo dispuesto en el artículo 6 de la citada Ley le corresponde, entre otros realizar investigación científica, formación y capacitación de recursos humanos y presentación de servicios de atención médica de alta especialidad, a través de estudios e investigaciones clínicas y experimentales de desarrollo tecnológico y básicas, en las áreas biomédicas y socioeconómicas de la población infantil y hasta la adolescencia, para lo cual requiere de espacio y estructuras adecuadas y suficientes que permiten el desarrollo funcional de las áreas médicas y administrativa

.

El INP es legalmente identificable mediante el Registro Federal de Contribuyentes INP8304203F7 con domicilio fiscal ubicado en Av. Insurgentes Sur 3700-Letra C, Colonia Insurgentes Cuicuilco, Alcaldía Coyoacán, Código Postal 04530 Ciudad de México, CDMX Teléfonos de contacto: 55 1084 0900, o Sitio web https://www.pediatria.gob.mx/

# V. Ámbito de Aplicación y Alcance del Documento de Seguridad.

En atención a los deberes contenidos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, el presente documento es aplicable para todas las unidades administrativas del Instituto Nacional de Pediatría que dan tratamiento a datos personales, en el ejercicio de sus atribuciones, facultades y funciones, sea en sistemas físicos o electrónicos, con independencia de la forma o modalidad de su creación, procesamiento, almacenamiento y organización. de forma completa o solo en un tramo del tratamiento por los datos personales que les corresponda.

Los datos personales pueden obrar en forma numérica, alfabética, gráfica, alfanumérica, fotográfica, sonora o en cualquier otro formato adquirido, generado, transformado, en cualquier soporte, sea escrito, óptico, impreso, sonoro, visual, audiovisual, electrónico, informático u holográfico, durante el desempeño de sus funciones y actividades en el INP.

El personal y servidores públicos que tengan acceso a los datos personales con motivo de su empleo, cargo o comisión, están obligados a conocer y aplicar las medidas de seguridad propias de cada sistema en él se involucre su actividad, y que concentre los datos personales, en todas y cada una de las fases del tratamiento de los mismos, partiendo desde la obtención y concluyendo con su eliminación.

Cabe señalar que para las obligaciones de confidencialidad se estableció un documento denominado **“ACUERDO DE CONFIDENCIALIDAD Y TRATAMIENTO DE DATOS PERSONALES “**donde se establece puntualmente cada una de los deberes y obligaciones a cumplir, las cuales subsistirán aún después de que haya finalizado su participación en el tratamiento de los datos personales, sea porque hayan cambiado de funciones e inclusive cuando la relación laboral o prestación del servicio con esta Entidad haya concluido.

# VI. Medidas de Apremio y Sanciones.

El incumplimiento a lo establecido en el Documento de Seguridad, así como en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales de Protección de Datos Personales para el Sector Público, será causa de la aplicación de medidas de apremio y/o sanciones correspondientes en los términos de dicha normatividad.

La Ley General en su Capítulo I, De las Medidas de Apremio, establece que el INAI puede aplicar las siguientes medidas de apremio a los responsables del sector público, para asegurar el cumplimiento de sus determinaciones:

- La amonestación pública, o
- La multa, equivalente a la cantidad de ciento cincuenta hasta mil quinientas veces el valor diario de la Unidad de Medida y Actualización.

El incumplimiento de los responsables será difundido en el portal de obligaciones de transparencia del INAI y considerados en las evaluaciones que se realicen.

Las medidas de apremio serán aplicadas por el INAI o con el apoyo de la autoridad competente, de conformidad con los procedimientos que establezcan las leyes respectivas

Para calificar las medidas de apremio el INAI considerara:

**I.** La gravedad de la falta del responsable, determinada por elementos tales como el daño causado; los indicios de intencionalidad; la duración del incumplimiento de las determinaciones del Instituto o los Organismos garantes y la afectación al ejercicio de sus atribuciones;

**II.** La condición económica del infractor, y

**III.** La reincidencia.

Las medidas de apremio deberán aplicarse e implementarse en un plazo máximo de quince días, contados a partir de que sea notificada la medida de apremio al infractor.

La amonestación pública será impuesta por el INAI y será ejecutada por el superior jerárquico inmediato del infractor con el que se relacione.

El INAI podrán requerir al infractor la información necesaria para determinar su condición económica, apercibido de que en caso de no proporcionar la misma, las multas se cuantificarán con base a los elementos que se tengan a disposición, entendidos como los que se encuentren en los registros públicos, los que contengan medios de información o sus propias páginas de Internet y, en general, cualquiera que evidencie su condición, quedando facultado el Instituto o los Organismos garantes para requerir aquella documentación que se considere indispensable para tal efecto a las autoridades competentes.

Las medidas de apremio de carácter económico no podrán ser cubiertas con recursos públicos.

En contra de la imposición de medidas de apremio, procede el recurso correspondiente ante el Poder Judicial de la Federación, o en su caso ante el Poder Judicial correspondiente en las Entidades Federativas

Asimismo, la Ley General dentro del Capítulo II de las Sanciones, establece las conductas que serán causa de sanción, entre otras:

**Artículo 163.** Serán causas de sanción por incumplimiento de las obligaciones establecidas en la materia de la presente Ley, las siguientes:

**I.** Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO;

**II.** Incumplir los plazos de atención previstos en la presente Ley para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate;

**III.** Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;

IV. Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la presente Ley;

V. No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos a que refiere el artículo 27 de la presente Ley, según sea el caso, y demás disposiciones que resulten aplicables en la materia;

VI. Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables. La sanción sólo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales;

VII. Incumplir el deber de confidencialidad establecido en el artículo 42 de la presente Ley;

VIII. No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la presente Ley;

IX. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad según los artículos 31, 32 y 33 de la presente Ley;

X. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la presente Ley;

XI. Obstruir los actos de verificación de la autoridad;

XII. Crear bases de datos personales en contravención a lo dispuesto por el artículo 5 de la presente Ley;

XIII. No acatar las resoluciones emitidas por el Instituto y los Organismos garantes, y

XIV. Omitir la entrega del informe anual y demás informes a que se refiere el artículo 44, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, o bien, entregar el mismo de manera extemporánea.

Las causas de responsabilidad previstas en las fracciones I, II, IV, VI, X, XII, y XIV, así como la reincidencia en las conductas previstas en el resto de las fracciones de este artículo, serán consideradas como graves para efectos de su sanción administrativa

Las responsabilidades que resulten de los procedimientos administrativos correspondientes, derivados de la violación a lo dispuesto por el artículo 163 de esta Ley, son independientes de las del orden civil, penal o de cualquier otro tipo que se puedan derivar de los mismos hechos.

Dichas responsabilidades se determinarán, en forma autónoma, a través de los procedimientos previstos en las leyes aplicables y las sanciones que, en su caso, se impongan por las autoridades competentes, también se ejecutarán de manera independiente.

Para tales efectos, el Instituto o los organismos garantes podrán denunciar ante las autoridades competentes cualquier acto u omisión violatoria de esta Ley y aportar las pruebas que consideren pertinentes, en los términos de las leyes aplicables.

En aquellos casos en que el presunto infractor tenga la calidad de servidor público, el Instituto o el organismo garante, deberá remitir a la autoridad competente, junto con la denuncia correspondiente, un Expediente en que se contengan todos los elementos que sustenten la presunta responsabilidad administrativa.

A efecto de sustanciar el procedimiento citado el INAI, deberá elaborar una denuncia dirigida a la contraloría, órgano interno de control o equivalente, con la descripción precisa de los actos u omisiones que, a su consideración, repercuten en la adecuada aplicación de la presente Ley y que pudieran constituir una posible responsabilidad.

Asimismo, deberá elaborar un expediente que contenga todos aquellos elementos de prueba que considere pertinentes para sustentar la existencia de la posible responsabilidad. Para tal efecto, se deberá acreditar el nexo causal existente entre los hechos controvertidos y las pruebas presentadas.

# **VII.** Responsabilidades, Funciones y Obligaciones de los Involucrados en el Tratamiento de Datos Personales en el INP.

Las Unidades Administrativas obligadas al cumplimiento del presente Documento de Seguridad, conforme al CAPITUTLO PRIMERO, DISPOSICIONES GENERALES, artículo 4° del Estatuto Orgánico de Instituto Nacional de Pediatría, son las siguientes:

Artículo 4°. Para el cumplimiento de su objeto y desempeño de las atribuciones que le competen, el Instituto contará con los siguientes órganos, unidades y comités

### Unidades Administrativas:

### a) Direcciones:

Dirección Médica.

Dirección de Investigación.

Dirección de Enseñanza.

Dirección de Administración.

Dirección de Planeación.

### b) Subdirecciones:

Subdirección de Medicina.

Subdirección de Cirugía.

Subdirección de Servicios

Auxiliares de Diagnóstico y Tratamiento.

Subdirección de Consulta Externa.

Subdirección de Medicina Crítica.

Subdirección de Hemato-Oncología

Subdirección de Enfermería

Subdirección de Investigación Médica.

Subdirección de Medicina Experimental.

Subdirección de Tecnologías de la Información.

Subdirección de Programación y Evaluación Educativa.

Subdirección de Administración y Desarrollo de Personal.

Subdirección de Finanzas.

Subdirección de Recursos Materiales.

Subdirección de Servicios Generales.

Subdirección de Asuntos Jurídicos

De acuerdo con lo previsto en el artículo 33, fracción II de la Ley General, el responsable debe definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales, para implementar y mantener medidas de seguridad para la protección de los datos personales; mismo que forma parte del documento de seguridad.

El artículo 57 de los Lineamientos, establece lo siguiente:

Funciones y obligaciones.

**Artículo 57.** Con relación a lo dispuesto en el artículo 33, fracción II de la Ley General, el responsable deberá establecer y documentar los roles y responsabilidades, así como la cadena de rendición de cuentas de todas las personas que traten datos personales en su organización, conforme al sistema de gestión implementado.

El responsable deberá establecer mecanismos para asegurar que todas las personas involucradas en el tratamiento de datos personales en su organización, conozcan sus funciones para el cumplimiento de los objetivos del sistema de gestión, así como las consecuencias de su incumplimiento.

Tomando en cuenta lo establecido en el artículo referido, las funciones y obligaciones del personal del INP que trata datos personales se han identificado en los siguientes perfiles:

## POLITICA INTERNA QUE ESTABLECE Y DOCUMENTA LOS PERFILES O ROLES DE LAS PERSONAS QUE LLEVAN A CABO TRATAMIENTO DE DATOS PERSONALES EN EL INP.

Tomando en consideración lo dispuesto en los artículos 56, fracción II y 57 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, se establecen y documentan los perfiles o roles y responsabilidades de las personas internas y externas del INP, involucradas con los tratamientos de datos personales que se efectúan, así como la cadena de rendición de cuentas correspondiente, conforme a lo siguiente:

| PERFIL O ROL | FIGURA | RESPONSABILIDAD |
|---|---|---|
| Responsable | Sujetos Obligados | Los sujetos obligados a que se refiere el artículo 1° de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y quien **define** quienes realizaran los tratamientos de datos personales de acuerdo con facultades y atribuciones. |
| Encargado | Persona física o moral que trata datos personales a nombre y cuenta del responsable | La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras **tratara** datos personales a nombre y cuenta del responsable. |
| Propietario del Sistema | Titular de la Unidad Administrativa | La persona que **genera** la información y decide sobre cómo se realiza el tratamiento de los datos personales que tiene asignados, conforme a facultades y atribuciones previstas en el Estatuto Orgánico del Instituto. |
| Administrador | Persona designada por el propietario del sistema que puede tomar decisiones respecto al uso y tratamiento de la información | La persona responsable de **otorgar** permisos y vigilar la ejecución de actividades asignadas a los usuarios. genéricos. |

| | | |
|---|---|---|
| Custodio | Persona que tiene a encargo el sistema de tratamiento de datos personales. | La persona que se **encarga** de la gestión de activos informáticos, su administración diaria y el monitoreo de la seguridad en los sistemas de tratamiento de datos personales que se encuentran bajo su resguardo |
| Usuario Genérico | Perona que realiza tratamiento de datos personales en los sistemas, a partir de privilegios otorgados. | La persona que utiliza el sistema de tratamiento de datos personales para interactuar con la información del sistema y realizar sus actividades, atendiendo a las medidas de seguridad específicas como son Confidencialidad, Integridad y Disponibilidad de la Información |

De esta forma a través de la estructura organizacional se tiene definida una cadena de rendición de cuenta y responsabilidad para poder asegurar que todo aquel que trate datos personales tenga claro que se encuentra involucrado en el logro de los cumplimientos institucionales en la materia, así como las consecuencias de su incumplimiento.

# VIII. Capítulo 1. Inventario de Datos Personales y de los Sistemas de Tratamiento.

Inventario de datos personales y sistemas de tratamiento De acuerdo con lo previsto en los artículos 33, fracción III y 35 de la Ley General, el responsable debe elaborar un inventario de datos personales y de los sistemas de tratamiento, para implementar y mantener medidas de seguridad para la protección de los datos personales; mismo que forma parte del documento de seguridad.

Los artículos 58 y 59 de los Lineamientos, establecen lo siguiente:

### Inventario de datos personales.

**Artículo 58.** Con relación a lo previsto en el artículo 33, fracción III de la Ley General, el responsable deberá elaborar un inventario con la información básica de cada tratamiento de datos personales, considerando, al menos, los siguientes elementos:

I. El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales; II. Las finalidades de cada tratamiento de datos personales;

III. El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no;

IV. El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales;

V. La lista de servidores públicos que tienen acceso a los sistemas de tratamiento;

VI. 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

VII. En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican éstas.

## Ciclo de vida de los datos personales en el inventario de éstos.

**Artículo 59.** Aunado a lo dispuesto en el artículo anterior de los presentes Lineamientos generales, en la elaboración del inventario de datos personales el responsable deberá considerar el ciclo de vida de los datos personales conforme lo siguiente:

I. La obtención de los datos personales;
II. El almacenamiento de los datos personales;
III. 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;
IV. La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen; V. El bloqueo de los datos personales, en su caso, y
V. La cancelación, supresión o destrucción de los datos personales.

Tomando en cuenta lo establecido en los artículos referidos, el Instituto Nacional de Pediatría, implementó un formulario con 25 contenidos, a través del cual se llevó a cabo el levantamiento de información de las unidades administrativa conforme a lo siguiente:

| 0. NÚMERO Y NOMBRE DEL ÁREA O UNIDAD ADMINISTRATIVA | Fecha de Elaboración (mes y año)<br>Fecha última Actualización (mes y año) |
|---|---|
| 1. Nombre del Sistema | |
| 2. Objetivo | |
| 3. Fundamento Legal | Indicar el fundamento legal que faculta al responsable para llevar a cabo el tratamiento, indicando los artículos, apartados, fracciones, incisos y nombre de los ordenamientos o disposición normativa vigente que le confiere atribuciones para realizar el tratamiento de datos personales, precisando su fecha de publicación o, en su caso, de la última reforma o modificación. |

**4. DATOS PERSONALES QUE CONTIENE EL SISTEMA (**Indicar todos los datos personales que son solicitados y que se contienen en el sistema)

- **I. Datos de identificación y autentificación** (nombre, domicilio, teléfono fijo y/o celular, correo electrónico personal, estado civil, firma, firma electrónica, cartilla militar, pasaporte lugar y fecha de nacimiento, nacionalidad, edad, fotografía, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), código bidimensional QR idiomas, fotografía), documento de nacionalización, cédula de identificación de extranjeros, acta de nacimiento del titular, actas expedidas por el registro civil, comprobantes de domicilio, nombre de beneficiarios designados,

- **II. Datos laborales** (empleos desempeñados, actividades extracurriculares, referencias laborales, referencias personales, recomendaciones, capacitaciones, cursos, idiomas documentos de selección, reclutamiento, nombramiento, incidencias, hojas de servicio, incapacidades, cuidados, gastos médicos mayores, estado cuenta AFORE, expedientes electrónico Único del ISSSTE, cuidados maternos inscripción al ISSSTE, baja del ISSSTE, tramites de jubilación, pensión, actas administrativas, licencias, documento de renuncia, documento de cese. credencial, medidas disciplinarias.

- **III. Datos de contacto y ubicación** (domicilio, teléfono fijo y/o celular, correo electrónico, redes sociales)

- **IV. Datos Académicos** (trayectoria académica y formación profesional como son calificaciones, boletas, constancia máxima de estudios, certificados, reconocimientos, títulos, cédulas profesionales)

- **V. Datos relacionados con intereses personales y profesionales** (pasatiempos, cursos, talleres)

- **VI. Datos patrimoniales o financieros** (bienes muebles e inmuebles, ingresos y egresos, cuentas bancarias, seguros, afores, historial crediticio, información fiscal, referencias personales crediticias, póliza de seguro de gastos médicos mayores para extranjeros, número de cuenta bancaria, clave / interbancaria, declaración patrimonial, prestaciones laborales, descuentos, cuotas sindicales, placa, modelo y marca de vehículo, créditos personales, datos de equipo de cómputo propio, marca, modelo, serie, solicitud de potenciación de seguro de vida )

- **VII. Datos biométricos** (relacionados con las características físicas, fisiológicas, huellas dactilares, los modelos retínales, la estructura facial, voces, geometría de la mano, color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros

- **VIII. Datos genéticos** (muestras genéticas tejidos o sangre, funciones de ciertos genes, muestras de ADN)

- **IX. Datos genómicos** (estructura y función del genoma de un organismo, secuencia de moléculas en los genes de un organismo, proteínas, ARN

- **X. Datos de salud** (estado de salud física o mental, historial clínico, alergias, enfermedades, información relacionada con cuestiones psicológicas o psiquiátricas, incapacidades, intervenciones quirúrgicas, vacunas, certificados o estudios médicos, consumo de sustancias toxicas, uso de aparatos ortopédicos, oftalmológicos, auditivos, prótesis)

☐ **XI. Datos ideológicos** (origen racial o étnico; estado de salud pasado, presente y futuro; información genética; creencias religiosas, filosóficas y morales; afiliación sindical; opiniones políticas y preferencia sexual.

☐ **XII. Datos de tránsito o migratorios** (Información sobre nacionalidad y su estadía dentro y fuera de país)

☐ **XIII. Aparatos de asistencia o apoyos funcionales** (de ortesis, prótesis y ayudas técnicas)

☐ **XIV. Datos sobre procedimientos administrativos relativos a una persona que se encuentre sujeta a un procedimiento seguido en forma de juicio.**

☐ En caso de recabar algún dato distinto, favor de indicarlo

_____

**5. FINALIDADES PARA LOS QUE SON TRATADOS LOS DATOS PERSONALES RECABADOS Y SI REQUIERE CONSENTIMIENTO**

Indicar cuales son las finalidades que dan origen y son necesarias para llevar a cabo y mantener la relación jurídica entre el responsable y el titular. las finalidades deben ser concretas, licitas, explicitas y legítimas, relacionada con las atribuciones normativas conferidas.

☐ Integrar el registro de la bolsa de trabajo en línea
☐ Para atender, registrar, dar seguimiento, gestionar y contactarle en relación a la(s) solicitud(es) que realice, para ocupar alguna plaza vacante.
☐ Para integrar registro de los interesados en participar en cursos de capacitación
☐ Para dar cumplimiento y seguimiento a las bases, requisitos y procedimientos para la admisión
☐ Para validar la veracidad y calidad de la información proporcionada por usted.
☐ Para dar continuidad al proceso de admisión.
☐ Para gestionar la aplicación del estudio psicométrico y de admisión que correspondan
☐ Para la aplicación de exámenes de admisión.
☐ Para informarle sobre los resultados de sus exámenes.
☐ Para realizar reportes estadísticos, previa aplicación de un mecanismo de disociación de los datos personales
☐ En caso de existir finalidad distinta, favor de indicarla_____

☐ Gestionar la recepción, expedición y entrega de los documentos físicos y/o digitales que acrediten a la persona interesada.
☐ Para realizar todos los trámites necesarios ante las autoridades correspondientes
☐ Para generar el Formato Único de Movimiento de Personal
☐ Para integrar el expediente de personal en cumplimiento a las disposiciones.
☐ Para identificación, y autentificación como Empleado y/o Servidor Público.
☐ Para generar y administrar credenciales para el acceso a las instalaciones
☐ Para generar los pagos y prestaciones correspondientes
☐ Para realizar trámites de altas, bajas y/o modificaciones ante el ISSSTE
☐ Para la administración del acceso electrónico (contraseñas) a los sistemas, aplicativos e infraestructura tecnológica.
☐ Para preservar la seguridad de las personas usuarias y las instalaciones, durante su ingreso y permanencia en el inmueble
☐ Para la elaboración hojas de servicios
☐ Para el descuento de préstamos, primas de seguro, pensión alimenticia
☐ Para contratación, de los seguros necesarios
☐ Para el cumplimiento de disposiciones fiscales
☐ Para el alta o baja en instituciones de seguridad social.
☐ Para la gestión de una cuenta bancaria que el interesado deberá realizar y comunicar a la cual se transfiera el pago de sueldos, salarios y prestaciones, en su caso.
☐ Para la integración de información relacionada con el estado de salud, incapacidades y licencias
☐ Para el otorgamiento de becas, premios, estímulos o recompensas.
☐ Para gestiones relacionados con procesos de certificación
☐ Para monitoreo en las cámaras de seguridad, circuito cerrado y grabaciones, así como para registro de asistencia
☐ Para evidenciar la organización de eventos compartiendo imágenes y fotografías
☐ Para realizar gestiones de los prestadores de Servicio Social y Prácticas Profesionales
☐ Para la celebración de instrumentos jurídicos en materia laboral
☐ Para efectos de control, auditoria y fiscalización que deriven de la relación laboral
☐ Para evaluar su desempeño

- Para comunicar la implementación de políticas y programas
- En caso de solicitarlo, para inscribirle y participar en cursos, talleres, programas y cualquier tipo de evento
- Para la emisión de constancias y demás reconocimientos correspondientes.
- Para contactar a sus familiares o terceros señalados como contacto en caso de una emergencia
- Para tramites de facturación
- Para realizar estudios de mercado en el caso de procedimientos de contratación que así lo requieran
- Para integración de expedientes de propuestas legal, técnica y económica en procesos de contratación, concesión, contratos, convenios, permisos, licencias o autorizaciones otorgados, procedimientos de adjudicación directa, invitación restringida y licitación de cualquier naturaleza, según sea el caso
- Para la elaboración de actas derivadas de procedimiento de contratación aplicable
- Para la elaboración de contratos en caso de ser adjudicado
- Para integrar y actualizar directorio de contratistas en caso de personas físicas
- Para atender requerimientos de autoridad
- Para realizar reportes estadísticos previa aplicación de un mecanismo de disociación de los datos personales.
- Para informarle de alguna vacante
- Para informarme sobre futuros eventos realizados por el Instituto o en colaboración.
- Para llevar el registro de asistencia en el caso de cursos de capacitación
- Para aquellos eventos, capacitaciones o pláticas informativas que impliquen el uso de plataforma de videoconferencia o diversos medios electrónicos, se grabarán las sesiones, a fin de documentar las sesiones como evidencia de su realización, quedando documentada la imagen y registro de voz de las y los participantes de esta
- Para conocer las necesidades de capacitación
- En caso de existir finalidad distinta, favor de indicarla _____

| Requiere consentimiento | Supuesto artículo 22, que se actualiza en su caso | Tipo de consentimiento |
|---|---|---|
| - Si<br>- No | Artículo 22. El responsable no estará obligado a recabar el consentimiento del titular para el tratamiento de sus datos personales en los siguientes casos:<br>- I. Cuando una ley así lo disponga, debiendo dichos supuestos ser acordes con las bases, principios y disposiciones establecidos en esta Ley, en ningún caso, podrán contravenirla;<br>- II. Cuando las transferencias que se realicen entre responsables, sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;<br>- III. Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;<br>- IV. Para el reconocimiento o defensa de derechos del titular ante autoridad competente;<br>- V. Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;<br>- VI. Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;<br>- VII. Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico, la prestación de asistencia sanitaria;<br>- VIII. Cuando los datos personales figuren en fuentes de acceso público<br>- IX. Cuando los datos personales se sometan a un procedimiento previo de disociación, o<br>- X. Cuando el titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley en la materia | - Tácito<br>- Expreso<br>- Expreso por escrito |

| 6.FORMA DE OBTENCIÓN DE LOS DATOS PERSONALES (Indicar la forma en que se obtienen los datos personales que obran en el Sistema o bien si estos provienen de otro Sistema) | |
|---|---|
| ☐ Gráfico<br>☐ Electrónico<br>☐ Telefónico<br>☐ Audiovisual<br>☐ Óptico<br>☐ Sonoro<br>☐ En caso de existir otro medio no enlistado, favor de indicar cual<br>_____<br>_____ | **Directa** ☐<br>**Indirecta** (obtenida, creada, generada en algún otro sistema) ☐<br>**Señalar cual:** |

| **7. Responsable** Los sujetos obligados a que se refiere el artículo 1° de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y quien **define** quienes realizaran los tratamientos de datos personales de acuerdo con facultades y atribuciones. | |
|---|---|
| Nombre | INP |
| Cargo | |
| Área de adscripción | |
| Teléfono | 55 1084 0900 Exts. |
| Correo electrónico | @pediatria.gob.mx |
| Función | Descripción de las atribuciones con relación al tratamiento de los datos personales sistema |
| Obligación | Descripción de las responsabilidades en cuanto al tratamiento de los datos personales del sistema |

| **8. Encargado.** La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras **tratara** datos personales a nombre y cuenta del responsable. | |
|---|---|
| Nombre | |
| Cargo | |
| Área de adscripción | |
| Teléfono | |
| Correo electrónico | |
| Función | |
| Obligación | |

| **9. Propietario del Sistema** La persona que **genera** la información y decide sobre cómo se realiza el tratamiento de los datos personales que tiene asignados, conforme a facultades y atribuciones previstas en el Estatuto Orgánico del Instituto. | |
|---|---|
| Nombre | |
| Cargo | Subdirector de Tecnologías de la Información |
| Área de adscripción | |
| Teléfono | 55 1084 0900 Ext 1495 |
| Correo electrónico | mtovarc@pediatria.gob.mx |
| Función | Descripción de las atribuciones con relación al tratamiento de los datos personales sistema |
| Obligación | Descripción de las responsabilidades en cuanto al tratamiento de los datos personales del sistema |

| **10. Administrador** La persona responsable de **otorgar** permisos y vigilar la ejecución de actividades asignadas a los usuarios genéricos. | |
|---|---|
| Nombre | |
| Cargo | |
| Área de adscripción | |
| Teléfono | |
| Correo electrónico | |
| Función | |
| Obligación | |

| | |
|---|---|
| **11. Custodio** La persona que se **encarga** de la gestión de activos informáticos, su administración diaria y el monitoreo de la seguridad en los sistemas de tratamiento de datos personales que se encuentran bajo su resguardo. | |
| Nombre | |
| Cargo | |
| Área de adscripción | |
| Teléfono | |
| Correo electrónico | |
| Función | |
| Obligación | |
| **12. Usuario Genérico** La persona que **utiliza** el sistema de tratamiento de datos personales para interactuar con la información y realizar sus actividades, atendiendo a las medidas de seguridad, así como a la Confidencialidad, Integridad y Disponibilidad de la Información | |
| Nombre | |
| Cargo | |
| Área de adscripción | |
| Teléfono | |
| Correo electrónico | |
| Función | |

**13. Tipo de soporte de la base de datos y donde se ubica el mismo** (Deberá indicar las características del lugar donde se resguardan los soportes, se deberá otorgar información conforme lo siguiente:

a) **Para soportes físicos**, el sujeto obligado deberá incluir una descripción escrita con detalles sobre las características físicas de la oficina, almacén o bodega donde resguarda dichos soportes;

b) **Para soportes electrónicos**, la descripción ofrecida por el sujeto obligado deberá incluir un diagrama de la arquitectura de seguridad en el cual sea posible apreciar el flujo de datos a través de la o las redes electrónicas que interconectan los equipos (clientes, servidores, cortafuegos, unidades de almacenamiento, entre otros) del sistema. Además, deberá describir las medidas de seguridad física que ha implementado para la protección del centro de datos donde residen tales soportes, y

c) **En caso de que el sistema ocupe ambos tipos de soportes**, deberá presentar las descripciones correspondientes a cada uno, en términos de lo señalado en los incisos a) y b) anteriores)

- ☐ a) Físico _____
- ☐ b) Electrónico _____
- ☐ c) Ambos _____

**14. Realiza transferencias de datos personales** (Entiéndase como la comunicación de datos o entrega total o parcial de los mismos, a cualquier persona distinta a su titular, sea mediante el uso de medios físicos o electrónicos, tales como la interconexión de computadoras o bases de datos, acceso a redes de telecomunicación, así como a través de la utilización de cualquier otra tecnología que lo permita. En el ámbito de la Administración Pública Federal se tienen)

SI ☐ NO ☐
*Describir en que consiste la transferencia conforme a lo siguiente:

- ☐ 1. Interinstitucionales (Transmisiones de datos a dependencias y entidades de la APF. Entidades federativas y municipios)
- ☐ 2. Internacionales (Transmisiones gobiernos u organismos internacionales)
- ☐ 3. Con entes privados u organizaciones civiles públicas o privadas

| ¿Qué datos personales o categorías son transferidos? | ¿A quién son transferidos? | ¿Para qué finalidad son transferidos? |
|---|---|---|
| | | |

| | | |
|---|---|---|
| | | |
| **Se requiere consentimiento**<br><br>SI ☐ NO ☐ | | |
| **Supuestos artículos 22, 66 o 70 que se actualizan en su caso** | **Tipo de consentimiento que se requiere para la transferencia**<br><br>☐ Tácito<br><br>☐ Expreso por escrito | **La transferencia requiere la suscripción de cláusulas contractuales, convenios de colaboración u otro instrumento jurídico.**<br><br>☐ SI ☐ NO |
| **15. Portabilidad de datos** (Indicar si las características del sistema permiten apreciar un sistema de datos personales estructurado comúnmente utilizado.) | | |
| SI ☐ | NO ☐ | |
| **16. Difusión de datos personales** (Indicar si en el tratamiento se realiza la difusión de datos personales y su fundamentación) | | |
| SI ☐<br>Fundamento_____<br>_<br><br>_____<br><br>NO ☐ | | |
| **17. Nivel de protección que requieren los datos** (indicar el nivel aplicable, el cual estará determinado en base a los datos en posesión, siguiendo los criterios internacionales de seguridad para el resguardo eficaz de los mismos. Los niveles de seguridad responden a la mayor o menor necesidad de garantizar la integridad de los datos personales, conforme a lo siguiente) | | |
| ☐ A. **Nivel Básico. – I** Datos de identificación y autentificación, **II** Datos laborales, **III** Datos de contacto, **V.** Datos relacionados con intereses personales y profesionales | | |
| ☐ B. **Nivel Medio. - IV.** Datos académicos, **VI.** Datos patrimoniales o financieros, **XII.** Datos de tránsito o migratorios, **XIII.** Aparatos de asistencia o apoyos funcionales, **XIV.** Datos sobre procedimientos administrativos seguido en forma de juicio | | |
| ☐ C. **Nivel Alto. - VII.** Datos biométricos, **VIII.** Datos genéticos, **IX.** Datos genómicos, **X.** Datos de salud, **XI.** Datos ideológicos | | |
| **18. Actualización de la información contenida en el sistema (**indicar la frecuencia con que se actualiza la información directamente en la base de datos del sistema) | | |
| ☐ Diaria ☐ Bimestral Trimestral ☐ Semestral ☐ Anual ☐ Otra especificar _____ | | |
| **19. Número de titulares involucrados** | | |
| **20. Plazo de conservación de los datos personales** (indicar cuanto tiempo permanecerán los datos personales en el Sistema de Datos conforme a su vigencia y finalidad, es decir atendiendo al ciclo de vida del trámite o servicio por motivo del cual se obtuvieron, basado en los instrumentos de control archivístico, CADIDO y Cuadro General de Clasificación Archivística) | | |
| ☐ _____ años ☐ _____ meses ☐ _____ días Otro especificar_____ | | |

| Indicar Sección de archivos | Serie de archivo | Subserie de archivo en su caso |
|---|---|---|
| | | |

| **21. Medidas de Seguridad** (indicar los elementos de seguridad con que se cuenta y se abordan en tres modalidades tomando como base el estándar internacional ISO/IEC 27002:2005 que se refiere a mejores prácticas sobre seguridad de la información) | |
|---|---|
| Físicas | ☐ Portación de credencial institucional<br>☐ Acceso solo a áreas autorizadas<br>☐ Acceso a instalaciones con código numérico o de barras<br>☐ Acceso a instalaciones en base a dato biométrico<br>☐ Puertas con cerradura, cerrojos, chapas. etc.<br>☐ Control e identificación de equipos portátiles de usuarios<br>☐ Control e identificación de equipos portátiles de empleados trabajadores<br>☐ Control de llaves<br>☐ Control de apertura y cierre de puertas externas e internas<br>Otro especificar_____ |
| Administrativas | ☐ **Política de seguridad.** Directrices estratégicas en materia de seguridad de activos, gestión, soporte, alineadas a las atribuciones de las dependencias o entidades. Incluye la elaboración y emisión interna de políticas, entre otros documentos regulatorios del sujeto obligado. Indicar cuales_____<br><br>☐ **Cumplimiento de la normatividad.** Controles establecidos para evitar violaciones a obligaciones legales, como pueden ser obligaciones contractuales o la política de seguridad interna. Abarca, entre otros, la identificación y el cumplimiento de requerimientos tales como la legislación aplicable al sujeto obligado, los derechos de propiedad intelectual, la protección de datos personales y la privacidad de la información personal. **Indicar cuales**_____<br><br>☐ **Organización de la seguridad de la información.** Establecimiento de controles internos y externos a través de los cuales se gestione la seguridad de activos. Considera, entre otros aspectos, la organización interna, que a su vez se refiere al compromiso de la alta dirección y la designación de responsables, entre otros objetivos; asimismo, considera aspectos externos como la identificación de riesgos relacionados con terceros. **Indicar cuales**_____<br><br>☐ **Clasificación y control de activos.** Establecimiento de controles en materia de identificación, inventario, control de mobiliario clasificación, ciclo vital de los datos y valuación de activos conforme a la normatividad aplicable. **Indicar cuales**_____<br><br>☐ **Seguridad relacionada a los recursos humanos.** Controles orientados a que el personal conozca el alcance de sus responsabilidades respecto a la seguridad de activos, antes, durante y al finalizar la relación laboral. **Indicar cuales**_____<br><br>☐ **Administración de incidentes.** Implementación de controles enfocados a la gestión de incidentes presentes y futuros que puedan afectar la integridad, confidencialidad y disponibilidad de la información. Incluye temas como el |

| | |
|---|---|
| | reporte de eventos y debilidades de seguridad de la información. **Indicar cuales**_____<br><br>**Continuidad de las operaciones.** Establecimiento de medidas con el fin de contrarrestar las interrupciones graves de la operación y fallas mayores en los sistemas de información. Incluye planeación, implementación, prueba y mejora del plan de continuidad de la operación del sujeto obligado. **Indicar cuales**_____ |
| Técnicas | **Gestión de comunicaciones y operaciones**. Establecimiento de controles orientados a definir la operación correcta y segura de los medios de procesamiento de información, tanto para la gestión interna como la que se lleva a cabo con terceros. Incluye, entre otros aspectos, protección contra código malicioso y móvil, copias de seguridad, gestión de la seguridad de redes y manejo de medios de almacenamiento.<br><br>Indicar cuales_____<br><br>**Control de acceso**. Establecimiento de medidas para controlar el acceso a la información, activos e instalaciones por parte de los responsables autorizados para tal fin, considerando en ello, la protección contra la divulgación no autorizada de información. Abarca, entre otros temas, gestión de acceso de los usuarios, control de acceso a redes, control de acceso a sistemas operativos y control de acceso a las aplicaciones y a la información.<br><br>Indicar cuales_____<br><br>**Adquisición, desarrollo, uso y mantenimiento de sistemas de información**: Integración de controles de seguridad a los sistemas de información, desde su adquisición o desarrollo, durante su uso y mantenimiento, hasta su cancelación o baja definitiva. Considera procesamiento adecuado en las aplicaciones, controles criptográficos y seguridad de los archivos de sistema, entre otros.<br><br>Indicar cuales<br>_____ |
| **22. Acceso a instalaciones (**Indicar los elementos que se advierten en el sujeto obligado conforme a lo siguiente) | |
| 1. **Seguridad perimetral exterior** (las instalaciones del sujeto obligado)<br>¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones?<br>a) ¿Cómo las identifica?<br>b) ¿Cómo las autentifica?<br>c) ¿Cómo les autoriza el acceso?<br><br>2. **Seguridad perimetral interior** (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):<br>*¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema?*<br>*Para las personas que acceden a dichos espacios interiores:*<br>*a) ¿Cómo las identifica?*<br>*b) ¿Cómo las autentifica?*<br>*c) ¿Cómo les autoriza el acceso?* | |

Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de vídeo-vigilancia, entre otras medidas.

**23. Perfiles de usuario y contraseña (**Indicar en este rubro el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica, conforme a lo siguiente)

1. Modelo de control de acceso [alguno de los siguientes]:
a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
b) ¿Es discrecional (matriz de control de acceso)?
c) ¿Está basado en roles (perfiles) o grupos?
d) ¿Está basado en reglas?

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de datos personales:
a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?

4. Administración de perfiles de usuario y contraseñas:
a) ¿Quién da de alta nuevos perfiles?
b) ¿Quién autoriza la creación de nuevos perfiles?
c) ¿Se lleva registro de la creación de nuevos perfiles?

5. Acceso remoto al sistema de datos personales:
a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
c) ¿Cómo se evita el acceso remoto no autorizado?

**24. Bitácoras de acceso y operación cotidiana, seguridad aplicable (**Indicar en este rubro como se controla y evidencian el control de acceso y operación cotidiana, conforme a lo siguiente:)

| | |
|---|---|
| Soporte físico | **Ejemplo de medidas de seguridad aplicables a bitácoras para sistemas en soportes físicos, para indicar lo propio conforme a lo siguiente:**<br>El responsable del sistema procura un estricto control y registro conforme a lo siguiente:<br>1. Las autorizaciones emitidas para facultar el acceso a un servidor público a fin de que éste, en el ejercicio de sus funciones, pueda interactuar con uno o más de los sistemas a su cargo.<br>2. La asignación, actualización y reemplazo de las llaves que entrega a los autorizados para que éstos puedan abrir el mecanismo de apertura de la puerta en la zona de acceso restringido.<br>3. Las acciones que los autorizados llevan a cabo en el área de resguardo. Para ello, designa a un Encargado quien anota lo siguiente: Quién solicita el acceso, cuándo se lleva a cabo (fecha y hora de entrada y salida), la razón que lo motiva y número del expediente utilizado.<br>4. El préstamo de expedientes es asistido por un sistema de cómputo que utiliza códigos de barras en los gafetes del personal autorizado y en los expedientes.<br>5. El sistema de préstamo de expedientes genera una bitácora electrónica que se respalda diariamente en un servidor dentro del centro de cómputo |

| | |
|---|---|
| | que administra el área de informática. Su integridad se garantiza copiando dicha bitácora en un CD-R diariamente.<br>6. El Encargado del sistema es la persona designada para analizar la bitácora cada mes mediante una herramienta<br>adquirida para tal fin. |
| Soporte electrónico | **Ejemplo de medidas de seguridad aplicables a bitácoras para sistemas en soportes electrónicos, para indicar lo propio conforme a lo siguiente**:<br>1. El Responsable del sistema -en coordinación con las áreas de informática y seguridad de la información- lleva un estricto control y registro, conforme a lo siguiente:<br>a) Las bitácoras de eventos ocurridos a nivel sistema operativo en los equipos (servidores, cortafuegos, almacenamiento masivo) que habilitan la operación del sistema de datos personales. Entre otras, se generan bitácoras para desempeño del servidor: intentos de acceso (exitosos y fallidos); accesos denegados a usuarios y terminales; uso de herramientas para administración del servidor, y fecha y hora de los eventos anteriores.<br>b) Las bitácoras de eventos generados a nivel software aplicativo del sistema de datos personales. Entre otras, se generan bitácoras para mensajes de error; apertura, modificación y cierre de archivos; violaciones de seguridad detectadas por el software aplicativo, y fecha y hora de estos eventos.<br>c) Las bitácoras de eventos relativos a las actividades de usuarios (capturistas, Encargados, el propio responsable y el administrador del servidor) en su interacción con el sistema de datos personales. Entre otras, se generan bitácoras para: Archivos, servicios y recursos utilizados; intentos de acceso (exitosos y fallidos); comandos y operaciones iniciadas, y fecha y hora de dichos eventos.<br>d) El conjunto de bitácoras permiten registrar, entre otros, los siguientes datos: Quién accede a los datos personales, desde dónde y con qué; accesos (intentos exitosos y fallidos) y salidas; propósito del acceso (sólo para modificaciones en el software aplicativo); operaciones llevadas a cabo; datos personales (registros y campos) utilizados de la base de datos, y fecha y hora de estos eventos.<br>e) Las bitácoras arriba mencionadas están todas en soportes electrónicos y se almacenan al menos por dos años en CD-R. Se tiene una copia en el centro de datos y otra se lleva a una bóveda bancaria subcontratada también para los respaldos. |
| **25. Lugar de almacenamiento de las bitácoras y tiempo de conservación y conservación de integridad** (Indicar lugar donde reside la bitácora sea físico o electrónico y como se mantiene la integridad de las bitácoras, conforme a lo siguiente:) | |
| a) Se garantiza copiándolas en un servidor del centro de datos el cual las graba en CD-R.<br>b) Algunas se copian cada hora, otras a diario<br>c) La integridad de las copias se garantiza además con “resúmenes” creados por un algoritmo “digestor”.<br>d) Se cuenta con una herramienta de software que automatiza estas operaciones.<br><br>Especificarse si las áreas de informática y seguridad de la información han designado una persona que se encarga de realizar un análisis de las bitácoras generadas, conforme a lo siguiente:<br><br>a) Se cuenta con la ayuda de una herramienta informática adquirida para tal propósito.<br>b) Cada semana se llevan a cabo análisis de bitácoras, pero no de todas ellas. Depende de la bitácora y de las amenazas detectadas en el entorno. | |
| **26. Registro de incidentes** (En este rubro el sujeto obligado debe describir el procedimiento de atención de incidentes que tiene implementado y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, | |

ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso, conforme a lo siguiente;)

1. Los datos que deberá registrar son:
a) La persona que resolvió el incidente;
b) La metodología aplicada;
c) Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y
d) Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados.
2. Si el registro está en soporte físico o en soporte electrónico;
3. Cómo asegura la integridad de dicho registro, y
4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.

Ejemplo de procedimiento en caso de presentarse un incidente, para indicar lo propio conforme a lo siguiente:
a) El Encargado elabora y entrega un informe al responsable a más tardar al día siguiente de haber ocurrido el incidente. Dicho informe precisa los soportes físicos o electrónicos afectados y, en su caso, los recuperados.
b) El incidente se registra en una hoja de cálculo anotando quién resolvió el incidente y los soportes dañados y recuperados. Dicha hoja está protegida con una contraseña de acceso. Su integridad se garantiza generando y almacenando un resumen creado por un algoritmo digestor en un servidor del centro de datos y respaldándola en un CD-R después de registrar un incidente.
c) En caso de robo o extravío de datos personales, el responsable del sistema, al tener conocimiento del incidente, da vista al titular de la dependencia o entidad para su conocimiento y al titular del área jurídica o aquél que tenga facultades para presentar denuncias o querellas ante el Ministerio Público para que, en el ámbito de sus atribuciones, determine lo conducente
d) A no más de 3 días naturales de haber ocurrido el incidente, el responsable del sistema da aviso al público mediante un desplegado de prensa que difunde el hecho por diversos medios, según la gravedad del caso, a escala local, regional o nacional.
e) En caso de robo o extravío de datos personales, se alerta a los titulares de los datos afectados para que tomen sus precauciones ante el posible uso ilegal de su información. Para tal efecto, el responsable del sistema da aviso por escrito a dichos titulares, a más tardar cinco días naturales de haber ocurrido el incidente, recabando el acuse de recibo de esta notificación.
Adicionalmente, se da aviso por correo electrónico o por teléfono.

27. Procedimiento de respaldo y recuperación de datos (Indicar si es el caso donde los medios de respaldo con que se cuenta, siendo deseable al menos dos lugares distintos que cumplan con las condiciones de seguridad; o bien si se utiliza un espacio externo seguro para guardar de manera sistemática datos y respaldos, conforme a lo siguiente:)

1. Señalar si realiza respaldos completos, diferenciales o incrementales;
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad;
3. Cómo y dónde archiva esos medios, y
4. Quién es el responsable de realizar estas operaciones (el sujeto obligado o un tercero)

28. Plan de contingencia Indicar si se cuenta con un plan de contingencia y si este atiende conforme a lo siguiente:)

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.
2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia del mismo.
3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:
a) El tipo de sitio (caliente, tibio o frío);
b) Si el sitio es propio o sub contratado con un tercero;
c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio, y
d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.

El tipo de sitio **caliente, tibio o frío** se refiere a la infraestructura, el equipo y el software disponibles en el sitio alterno; por lo que a mayor disponibilidad de dichos elementos resulta una menor demora para restablecer las operaciones de uno o más sistemas. Ejemplos de lo anterior son, en cuanto a infraestructura: aire acondicionado, cableado, suministro de energía eléctrica y enlaces de comunicaciones; en cuanto al equipo: servidores, almacenamiento y periféricos, y por lo que se refiere al software: sistemas operativos, manejadores de bases de datos y aplicaciones. Por lo tanto:

i) **En un sitio alterno caliente** se mantienen disponibles en todo momento la infraestructura, el equipo y el software; lo único que hace falta para iniciar operaciones son los datos y el personal. Este tipo de sitios alternos es el más costoso, pero supone tan solo unas cuantas horas para restaurar operaciones.

ii) **El sitio alterno tibio** cuenta con infraestructura no configurada y equipos equivalentes que pueden estar disponibles en pocas horas, pero no contienen software ni datos. Este tipo de sitios alternos es el punto medio en costo y tiempo para restaurar operaciones.

iii) **El sitio alterno frío** cuenta con un ambiente mínimo de infraestructura y no cuenta con el equipo. Este tipo de sitios alternos es el menos costoso, pero supone demora de algunos días para restablecer operaciones.

**29. Encargado de datos (**Indicar el Prestador de servicios persona física o moral, pública o privada ajena al INP que sola o conjuntamente con otros, trata datos personales a nombre y por cuenta en subcontratación, conforme a lo siguiente:)

| | | | | |
|---|---|---|---|---|
| Existe un prestador de servicios, persona física o moral, pública o privada ajena al INP que sola o conjuntamente, trate datos personales a nombre y por cuenta de este Instituto | SI | | NO | |

**30. Plazo de conservación y bloqueo de los datos personales (**periodo en el que la autoridad conservará los datos para efectos de responsabilidades, el cual será equivalente al plazo de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento en términos de la normatividad de aplicable y, cumplido este plazo, deberá procederse a la supresión del dato que implica el borrado físico del mismo, conforme a las siguientes consideraciones:)

a) Deberá considerar lo dispuesto en el Catálogo de disposición documental -un registro general, además, que se debe incluir la siguiente información del Catálogo de disposición documental -un registro general y sistemático que establece los siguientes valores documentales-: (i) los plazos de conservación; (ir) la vigencia documental; (iii) la clasificación de reserva o confidencialidad, y (iv) el destino final de los documentos.

b) Deberá verificar si el mismo tiene valores históricos, científicos, estadísticos o contables. En caso de que contenga dichos valores, los datos personales serán objeto de transferencias secundarias, de conformidad con lo establecido por los catálogos de disposición documenta.

c) Deben atender al valor documental de la información contenida en el mismo, de conformidad con los criterios establecidos por el sujeto obligado en consideración a la posible consulta que de los mismos se requiriera o a cualquier otra implicación jurídica que pudiera existir en razón de la normatividad aplicable.

**3.** Doc.4_Versión**05**_170724_Formulario levantamiento inventario tratamiento datos personales.

# IX. Funciones y Obligaciones de las Personas que traten Datos Personales Previstos en el Inventario de Datos Personales y en los Sistemas de Tratamiento.

De forma general se establecen criterios generales de seguridad, de observancia obligatoria para todo el personal que, en Instituto Nacional de Pediatría, que detenta datos personales, con motivo de sus funciones.

**a)** Guardar la debida secrecía sobre los datos personales que conozcan en el desarrollo de sus funciones, evitando su difusión y/o transmisión.

**b)** Informar al responsable del sistema o responsable de la unidad administrativa o área. sobre cualquier incidencia que tenga conocimiento.

**c)** No dejar información visible cuando abandone su puesto, ya sea que se ausente de manera temporal o si hay alguna persona ajena a la Unidad Administrativa a la que esté adscrito.

**d)** Conservar el buen estado físico de los soportes documentales a que tengan acceso, por motivo del ejercicio de sus funciones.

**e)** Reportar alguna vulneración de los datos personales.

# X. Sistemas de Tratamiento por Unidad Administrativa.

# XI. Inventarios de Datos Personales y Sistemas.

# XII. Análisis de Riesgos.

Se realiza un análisis de riesgos del tratamiento de los datos personales de acuerdo a la siguiente metodología:

Los riesgos sobre el tratamiento de datos personales se detectan por área administrativa, académica o de servicio y por cualquier persona que dé tratamiento de datos personales.

Se realiza la "Matriz de Riesgos Por Tratamiento de Datos Personales donde se identifica:

### Tratamiento de datos personales.

Clave de tratamiento de datos personales conforme al inventario.

### Riesgo probable.

Enunciado del riesgo identificado, tomando en cuenta:

- Los requerimientos regulatorios, legales y reglamentarios.
- El valor de los datos personales de acuerdo a si son sensibles o no y su ciclo de vida;
- El valor y exposición de los activos involucrados en el tratamiento de los datos personales;
- Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida, y
- Los siguientes factores:
  - El riesgo inherente a los datos personales tratados;
  - La sensibilidad de los datos personales tratados;
  - El desarrollo tecnológico; o Las posibles consecuencias de una vulneración para los titulares;
  - Las transferencias de datos personales que se realicen;
  - El número de titulares;
  - Las vulneraciones previas ocurridas en los sistemas de tratamiento, y
  - 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.

## Causa probable.

La causa probable del riesgo. Pueden usarse las herramientas del análisis de causa raíz como los 5 por qué's, diagrama de Ishikawa, entre otros.

## Probabilidad.

La probabilidad subjetiva de que ocurra el riesgo. Es la posibilidad de que ocurra una vulneración de seguridad a los datos personales. Para determinar su probabilidad se toma en cuenta el número de áreas en las que se ha identificado el riesgo.

Criterio cuya escala es:

| PROBABILIDAD | ESCALA |
|---|---|
| De 1 a 3 áreas | Bajo |
| De 4 a 5 áreas | Medio |
| De 6 a 7 áreas | Alto |

## Impacto.

El impacto del riesgo se refiere al impacto a las consecuencias negativas, daño o afectación para los titulares que pudieran derivar de una vulneración de seguridad ocurrida en los datos personales. Criterio cuya escala es:

| IMPACTO | ESCALA |
|---|---|
| No impacta a la integridad, confidencialidad ni disponibilidad de datos personales. Bajo Impacta a la integridad, confidencialidad o disponibilidad de datos personales. Medio Impacta a la integridad, confidencialidad y disponibilidad de datos personales. | Bajo |
| No impacta a la integridad, confidencialidad ni disponibilidad de datos personales. Bajo Impacta a la integridad, confidencialidad o disponibilidad de datos personales. Medio Impacta a la integridad, confidencialidad y disponibilidad de datos personales. | Medio |
| No impacta a la integridad, confidencialidad ni disponibilidad de datos personales. Bajo Impacta a la integridad, confidencialidad o disponibilidad de datos personales. Medio Impacta a la integridad, confidencialidad y disponibilidad de datos personales. | Alto |

## Cálculo de Nivel de valor de Riesgo.

Para este caso, se asume que el Impacto y la Probabilidad tienen el mismo valor para la valuación del riesgo. Se identifica en la gráfica Probabilidad vs Impacto la zona en la que se encuentra el riesgo identificado para asignarle su nivel de valor de riesgo, que definirá la prioridad con la que se tratarán los riesgos, de la siguiente manera:

Una vez identificados los riesgos y su prioridad, se define el tratamiento del riesgo, el cual puede ser:

- Mitigar: acciones que minimicen los efectos que pudieran surgir por los riesgos.
- Eliminar: acciones que desaparezcan los efectos del riesgo.
- Transferir: acciones que trasladen el riesgo. Generalmente ocurre cuando no se tiene control total sobre la situación.
- Aceptar: Generalmente ocurre cuando no se tiene control total sobre la situación.

Una vez identificado el tratamiento del riesgo se plantean acciones para mitigar, eliminar, transferir o aceptar el riesgo, debiendo considerar los controles de seguridad física, administrativa y técnica para la protección de datos personales.

Cuando se identifique algún riesgo se debe notificar al Propietario del Sistema de Tratamiento para que la integre a la Matriz de Riesgos.

## Análisis de Brecha.

- El análisis de brecha considera los siguiente:
- Las medidas de seguridad existentes y efectivas;
- El nivel óptimo de medidas de seguridad y
- Las medidas de seguridad adicionales a las existentes para alcanzar el nivel óptimo.

| | |
|---|---|
| 0. SUBDIRECCION DE RECURSOS MATERIALES | Fecha de Elaboración (mes y año): Junio 2024<br>Fecha última Actualización (mes y año): Junio 2024 |
| 1. Nombre del Sistema | SISTEMA INTEGRAL DE ADMINISTRACIÓN INP |
| 2. Objetivo | Registrar, clasificar, asignar y controlar los procedimientos de Adquisiciones y sus derivados. |
| 3. Fundamento Legal | Constitución Política de los Estados Unidos Mexicanos, Art. 134<br>Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y su Reglamento.<br>Estatuto Orgánico del Instituto Nacional de Pediatría.<br>Políticas, Bases y Lineamientos en Materia de Adquisiciones del Instituto Nacional de Pediatría. |

**4. DATOS PERSONALES QUE CONTIENE EL SISTEMA** (Indicar todos los datos personales que son solicitados y que se contienen en el sistema)

☒ **I. Datos de identificación y autentificación** (nombre, domicilio, teléfono fijo y/o celular, correo electrónico personal, firma, firma electrónica, pasaporte lugar y fecha de nacimiento, nacionalidad, edad, fotografía, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), código bidimensional QR ), documento de nacionalización, cédula de identificación de extranjeros, acta de nacimiento del titular, actas expedidas por el registro civil, comprobantes de domicilio,

☐ **II. Datos laborales.** NO APLICA

☒ **III. Datos de contacto y ubicación** (domicilio, teléfono fijo y/o celular, correo electrónico,)

☐ **IV. Datos Académicos** . NO APLICA

☐ **V. Datos relacionados con intereses personales y profesionales** NO APLICA

☐ **VI. Datos patrimoniales o financieros** (cuentas bancarias, información fiscal)

☒ **VII. Datos biométricos** NO APLICA

☐ **VIII. Datos genéticos** NO APLICA

☐ **IX. Datos genómicos** NO APLICA

☐ **X. Datos de salud** NO APLICA

☐ **XI. Datos ideológicos** . NO APLICA

☐ **XII. Datos de tránsito o migratorios** NO APLICA

☐ **XIII. Aparatos de asistencia o apoyos funcionales** NO APLICA

☐ **XIV. Datos sobre procedimientos administrativos relativos a una persona que se encuentre sujeta a un procedimiento seguido en forma de juicio.** NO APLICA

☐ En caso de recabar algún dato distinto, favor de indicarlo

---

**5. FINALIDADES PARA LOS QUE SON TRATADOS LOS DATOS PERSONALES RECABADOS Y SI REQUIERE CONSENTIMIENTO**

Indicar cuales son las finalidades que dan origen y son necesarias para llevar a cabo y mantener la relación jurídica entre el responsable y el titular. las finalidades deben ser concretas, licitas, explicitas y legítimas, relacionada con las atribuciones normativas conferidas.

☒ Para dar cumplimiento a la normatividad vigente en los procesos de Adquisición, así como el registro de las actividades del mismo y los reportes derivados de ello.

| Requiere consentimiento | Supuesto artículo 22, que se actualiza en su caso | Tipo de consentimiento |
|---|---|---|
| ☐ Si<br>☒ No | Artículo 22. El responsable no estará obligado a recabar el consentimiento del titular para el tratamiento de sus datos personales en los siguientes casos:<br>☒ I. Cuando una ley así lo disponga, debiendo dichos supuestos ser acordes con las bases, principios y disposiciones establecidos en esta Ley, en ningún caso, podrán contravenirla;<br>☐ II. Cuando las transferencias que se realicen entre responsables, sean sobre datos personales que se | ☒ Tácito<br>☐ Expreso<br>☐ Expreso por escrito |

| | | |
|---|---|---|
| | utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;<br>☐ III. Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;<br>☐ IV. Para el reconocimiento o defensa de derechos del titular ante autoridad competente;<br>☐ V. Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;<br>☐ VI. Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;<br>☐ VII. Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico, la prestación de asistencia sanitaria;<br>☐ VIII. Cuando los datos personales figuren en fuentes de acceso público<br>☐ IX. Cuando los datos personales se sometan a un procedimiento previo de disociación, o<br>☐ X. Cuando el titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley en la materia. | |

**6.FORMA DE OBTENCIÓN DE LOS DATOS PERSONALES** (Indicar la forma en que se obtienen los datos personales que obran en el Sistema o bien si estos provienen de otro Sistema)

| | | |
|---|---|---|
| ✖ Grafico<br>✖ Electrónico<br>☐ Telefónico<br>☐ Audiovisual<br>☐ Óptico<br>☐ Sonoro<br>☐ En caso de existir otro medio no enlistado, favor de indicar cual<br>_____ | Directo ✖ | **Indirecta** (obtenida, creada, generada en algún otro sistema) ☐<br>**Señalar cual:** |

**7. Responsable del Sistema** Se entiende a la persona Titular de la Unidad Administrativa propietaria del Sistema

| | |
|---|---|
| Nombre | Lic. José Luis Martínez Aguilar |
| Cargo | Encargado de la Sub. de Recursos Materiales |
| Área de adscripción | Subdirección de Recursos Materiales |
| Teléfono | 55 1084 0900 Exts. 1408 y 1105 |
| Correo electrónico | jmartineza@pediatria.gob.mx |
| Función | Descripción de las atribuciones con relación al tratamiento de los datos personales sistema |
| Obligación | Descripción de las responsabilidades en cuanto al tratamiento de los datos personales del sistema. |

**8. Encargado.** La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras **tratara** datos personales a nombre y cuenta del responsable.

| | |
|---|---|
| Nombre | |
| Cargo | |
| Área de adscripción | |

| | |
|---|---|
| Teléfono | |
| Correo electrónico | |
| Función | |
| Obligación | |
| **9. Propietario del Sistema** La persona que **genera** la información y decide sobre cómo se realiza el tratamiento de los datos personales que tiene asignados, conforme a facultades y atribuciones previstas en el Estatuto Orgánico del Instituto. | |
| Nombre | |
| Cargo | |
| Área de adscripción | |
| Teléfono | |
| Correo electrónico | |
| Función | |
| Obligación | |
| **10. Administrador** La persona responsable de **otorgar** permisos y vigilar la ejecución de actividades asignadas a los usuarios genéricos. | |
| Nombre | |
| Cargo | |
| Área de adscripción | |
| Teléfono | |
| Correo electrónico | |
| Función | |
| Obligación | |
| **11. Custodio** La persona que se **encarga** de la gestión de activos informáticos, su administración diaria y el monitoreo de la seguridad en los sistemas de tratamiento de datos personales que se encuentran bajo su resguardo. | |
| Nombre | Ing. Misael Teófilo Tovar Cruz |
| Cargo | Subdirector de Tecnologías de la Información |
| Área de adscripción | Dirección de Planeación |
| Teléfono | 55 1084 0900 Ext 1495 |
| Correo electrónico | mtovarc@pediatria.gob.mx |
| Función | Protección de datos, implementar medidas de seguridad, gestionar incidentes, promover la conciencia de seguridad. Mantener la protección adecuada de la información confidencial.<br><br>Mantener la disponibilidad, confidencialidad e integridad en los datos personales e institucionales. |
| Obligación | Articulo 3.- Numero VIII. Atender las disposiciones normativas en materia de protección de datos personales, transparencia y rendición de cuentas;<br><br>e) Considerar medidas de rescisión y/o responsabilidades legales en caso de que los proveedores o su personal transgredan las políticas y acuerdos de confidencialidad o realicen actividades que, sin<br>autorización de la Institución, expongan la información institucional o incumplan con la legislación en<br>materia de protección de datos personales.<br><br>Artículo 67.- Los proyectos de servicios de desarrollo o mantenimiento de software deberán incluir el diseño detallado o conceptual del aplicativo a desarrollar, que comprenda por lo menos:<br><br>c) Políticas de privacidad y protección de datos personales, de conformidad con la legislación aplicable;<br><br>Artículo 69.- Los aplicativos de cómputo que operen sobre datos críticos, confidenciales o sensibles, deberán garantizar que el procesamiento y transferencia de la información se realice a través de mecanismos que garanticen su seguridad e integridad, como priorizar su alojamiento en territorio nacional. Para ello, deberán atender los Estándares Técnicos emitidos por la CEDN, la legislación en materia de protección de datos personales y las disposiciones que sean emitidas en materia de Seguridad Nacional. |
| **12. Usuarios u Operador del Sistema** (Se anexa listado) | |

**13. Tipo de soporte de la base de datos y donde se ubica el mismo** (Deberá indicar las características del lugar donde se resguardan los soportes, se deberá otorgar información conforme lo siguiente:
a) **Para soportes físicos**, el sujeto obligado deberá incluir una descripción escrita con detalles sobre las características físicas de la oficina, almacén o bodega donde resguarda dichos soportes;

b) **Para soportes electrónicos**, la descripción ofrecida por el sujeto obligado deberá incluir un diagrama de la arquitectura de seguridad en el cual sea posible apreciar el flujo de datos a través de la o las redes electrónicas que interconectan los equipos (clientes, servidores, cortafuegos, unidades de almacenamiento, entre otros) del sistema. Además, deberá describir las medidas de seguridad física que ha implementado para la protección del centro de datos donde residen tales soportes, y

c) **En caso de que el sistema ocupe ambos tipos de soportes**, deberá presentar las descripciones correspondientes a cada uno, en términos de lo señalado en los incisos a) y b) anteriores)

- ☐ d) Físico
- ☐ e) Electrónico
- ✖ f) **Ambos** Oficina destinada al Archivo, misma que cuenta con anaqueles, archiveros y carpetas, Base de Datos del Sistema Integral de Administración, acceso restringido a la red institucional, cortafuegos, centro de datos principal con acceso controlado y restringido con biométrico dactilar, manejo de usuarios con contraseña bajo perfiles de usuario, antivirus, acceso al equipo de cómputo mediante Directorio Activo.

**14. Realiza transferencias de datos personales** (Entiéndase como la comunicación de datos o entrega total o parcial de los mismos, a cualquier persona distinta a su titular, sea mediante el uso de medios físicos o electrónicos, tales como la interconexión de computadoras o bases de datos, acceso a redes de telecomunicación, así como a través de la utilización de cualquier otra tecnología que lo permita. En el ámbito de la Administración Pública Federal se tienen)

SI ■ NO ✖

Describir en que consiste la transferencia conforme a lo siguiente:

- ☐ 4. Interinstitucionales (Transmisiones de datos a dependencias y entidades de la APF. Entidades federativas y municipios)
- ☐ 5. Internacionales (Transmisiones gobiernos u organismos internacionales)
- ☐ 6. Con antes privados u organizaciones civiles públicas o privadas.

| ¿Qué datos personales o categorías son transferidos? | ¿A quién son transferidos? | ¿Para qué finalidad son transferidos? |
|---|---|---|
| | | |

**Se requiere consentimiento**

SI ☐ NO ☐

| Supuestos artículos 22, 66 ó 70 que se actualizan en su caso | Tipo de consentimiento que se requiere para la transferencia | La transferencia requiere la suscripción de clausulas contractuales, convenios de colaboración u otro instrumento jurídico. |
|---|---|---|
| | ☐ Tácito<br>☐ Expreso por escrito | ☐ SI ☐ NO |

**15. Portabilidad de datos** (Indicar si las características del sistema permiten apreciar un sistema de datos personales estructurado comúnmente utilizado.)

| SI ☐ | NO ✖ |
|---|---|

**16. Difusión de datos personales** (Indicar si en el tratamiento se realiza la difusión de datos personales y su fundamentación)

SI ✖

Fundamento: Ley General de Transparencia y Acceso a la Información Pública, Art. 70 Fracc. 28ª 28b y 32

NO ☐

**17. Nivel de protección que requieren los datos** (indicar el nivel aplicable, el cual estará determinado en base a los datos en posesión, siguiendo los criterios internacionales de seguridad para el resguardo eficaz de los mismos. Los

niveles de seguridad responden a la mayor o menor necesidad de garantizar la integridad de los datos personales, conforme a lo siguiente)

✖ A. **Nivel Básico. – I** Datos de identificación y autentificación, **II** Datos laborales, **III** Datos de contacto, **V.** Datos relacionados con intereses personales y profesionales

☐ B. **Nivel Medio. - IV.** Datos académicos, **VI.** Datos patrimoniales o financieros, **XII**. Datos de tránsito o migratorios, **XIII.** Aparatos de asistencia o apoyos funcionales, **XIV.** Datos sobre procedimientos administrativos seguido en forma de juicio

☐ C. **Nivel Alto. - VII.** Datos biométricos, **VIII**. Datos genéticos, **IX.** Datos genómicos, **X.** Datos de salud, **XI.** Datos ideológicos

**18. Actualización de la información contenida en el sistema** (indicar la frecuencia con que se actualiza la información directamente en la base de datos del sistema)

✖ Diaria ☐ Bimestral Trimestral ☐ Semestral ☐ Anual ☐ Otra especificar

**19. Número de titulares involucrados:** 560 involucrados

**20. Plazo de conservación de los datos personales** (indicar cuanto tiempo permanecerán los datos personales en el Sistema de Datos conforme a su vigencia y finalidad, es decir atendiendo al ciclo de vida del trámite o servicio por motivo del cual se obtuvieron, basado en los instrumentos de control archivístico, CADIDO y Cuadro General de Clasificación Archivística)

INFORMACIÓN PROPORCINADA POR EL RESPONSABLE DEL ARCHIVO

✖ **6** años **(2 años en trámite y 4 años en concentración)** ☐ ____ meses ____☐_____ días Otro ☐

| Indicar Sección de archivos | Serie de archivo | Subserie de archivo en su caso |
|---|---|---|
| 6C | 6C.4 | |

**21. Medidas de Seguridad** (indicar los elementos de seguridad con que se cuenta y se abordan en tres modalidades tomando como base el estándar internacional ISO/IEC 27002:2005 que se refiere a mejores prácticas sobre seguridad de la información)

| | |
|---|---|
| Físicas | ✖ Portación de credencial institucional<br>✖ Acceso solo a áreas autorizadas<br>☐ Acceso a instalaciones con código numérico o de barras<br>✖ Acceso a instalaciones en base a dato biométrico<br>✖ Puertas con cerradura, cerrojos, chapas. Etc.<br>☐ Control e identificación de equipos portátiles de usuarios<br>✖ Control e identificación de equipos portátiles de empleados trabajadores<br>✖ Control de llaves<br>☐ Control de apertura y cierre de puertas externas e internas<br>Otro especificar_____ |
| Administrativas | ✖ **Política de seguridad.**: Código de Conducta, Código de Ética y Política general de Seguridad de la Información<br><br>☐ **Cumplimiento de la normatividad. Contrato de servicios y Acuerdo de confidencialidad**<br><br>☐ **Organización de la seguridad de la información.** Política de Seguridad de la información (Garantizar la confidencialidad, integridad y disponibilidad de la información del INP, a partir del establecimiento de lineamientos, políticas, controles, procedimientos y el fomento de una cultura de seguridad de la información.)<br><br>☐ **Seguridad relacionada a los recursos humanos.** Política De Recursos Humanos (Establecer los lineamientos, en materia de seguridad de la información, sobre el proceso de Recursos Humanos que deben pasar previo a la relación laboral, durante la relación laboral con el Instituto Nacional de Pediatría y una vez que se dé por terminada la relación laboral.)<br><br>☐ **Administración de incidentes.** Plan De Contingencia (Se establece el procedimiento de responsabilidades para la detección, escalado y mitigación de incidentes de seguridad de la información del sistema través de la Subdirección de TI).<br><br>✖ **Continuidad de las operaciones.** Política de Gestión (Establecer los lineamientos, en materia de seguridad de la información, para identificar, detectar, registrar, reportar y atender de forma adecuada y eficaz los incidentes de seguridad de la información con la finalidad de reducir el posible impacto de estos en las operaciones del INP.) Teniendo en cuenta el equipo de protección civil ante desastres naturales |

| | |
|---|---|
| Técnicas | **Gestión de comunicaciones y operaciones**. Política de tecnologías Móviles (Establece lineamientos, en materia de seguridad de la información, para prevenir pérdidas, daños, hurtos o el compromiso de los recursos tecnológicos, así como para la seguridad y protección de los equipos de escritorio y portátiles contra amenazas físicas y lógicas.), uso de perfiles de usuario y software antivirus<br><br>**Control de acceso**.<br>Política de administración de la seguridad de la red (Establece los lineamientos, en materia de seguridad de la información, sobre la administración de seguridad de la red y el acceso y restricción a las redes del INP, que permitan asegurar la confidencialidad, integridad y disponibilidad de la información que se transmite a través de estas), Directorio Activo, Perfiles de usuarios en sistemas informáticos<br><br>**Adquisición, desarrollo, uso y mantenimiento de sistemas de información**: Política de Sistemas, Aplicaciones y Servicios (Establece los lineamientos, en materia de seguridad de la información, para mantener la seguridad de la información durante la adquisición, desarrollo y mantenimiento de sistemas, así como establecer lineamientos a seguir por parte de los colaboradores del Instituto Nacional de Pediatría, para asegurar la integración de la seguridad de la información en los sistemas de información actuales y futuros que sean parte del INP.) |

**22. Acceso a instalaciones** (Indicar los elementos que se advierten en el sujeto obligado conforme a lo siguiente)1

1. **Seguridad perimetral exterior** (las instalaciones del sujeto obligado)
¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones?
Controles biométricos y portación de credencial

- **Personal que labora en el Instituto Nacional de Pediatría (INP)**

**Control de acceso biométrico de reconocimiento facial para el personal, portación de credencial Institucional, circuito cerrado de Televisión y personal de vigilancia que se idéntica visualmente con su uniforme**

- **Personal Externo al INP**

**Se cuenta con registro en ventanilla con el personal de vigilancia, se capturan sus datos y fotografía de la persona a ingresar y se comparte un código de tipo quick response que lo deben de portar durante su visita**

- **Registro de familiares del paciente**

**Se hace mediante el carnet del paciente**
¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones?
a) ¿Cómo las identifica? **El personal porta la credencial dentro de la institución,**
b) ¿Cómo las autentifica? **Con la inspección visual y monitoreo en el circuito cerrado**
c) ¿Cómo les autoriza el acceso? **Por medio del personal de seguridad cuando se porta la credencial**

2. **Seguridad perimetral interior** (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):
¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? **Se ingresa a partir de una puerta con control biométrico de huella dactilar al centro de datos principal y registro de bitácora, puertas con acceso restringido a los cuartos de comunicación secundarios**
Para las personas que acceden a dichos espacios interiores:
a) ¿Cómo las identifica? **El personal tiene la obligación de portar la credencial en todo momento, huella dactilar en el centro de datos y monitoreo mediante circuito cerrado**
b) ¿Cómo las autentifica? Existen perfiles de acceso al centro de datos por el reconocimiento dactilar, **Se cuenta con circuito cerrado en el hospital**
c) ¿Cómo les autoriza el acceso? **Se asigna al personal del Instituto, registra su entrada con biométrico en el centro de datos, existe una bitácora de acceso y se registra hora, nombre del personal que ingresa, hora de entrada, hora de salida y motivo del ingreso.**

**23. Perfiles de usuario y contraseña**

1. Modelo de control de acceso:
a) ¿Es obligatorio? **Si**
b) ¿Es discrecional? **Si**
c) ¿Está basado en roles (perfiles) o grupos? **Si**
d) ¿Está basado en reglas? **Sí**

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
a) ¿Cuenta con un sistema operativo de red instalado en sus equipos? **Sí**
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas? **Sí**
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? **Solo las contraseñas**

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de datos personales:
a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas? **Sí**
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? **Solo las contraseñas**

4. Administración de perfiles de usuario y contraseñas:
a) ¿Quién da de alta nuevos perfiles? **Administradores (Encargados) del sistema**
b) ¿Quién autoriza la creación de nuevos perfiles? **Jefe Inmediato del Área**
c) ¿Se lleva registro de la creación de nuevos perfiles? **Sí, mediante solicitud escrita**

5. Acceso remoto al sistema de datos personales:
a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? **No**
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? **No**
c) ¿Cómo se evita el acceso remoto no autorizado? **Por restricción de acceso mediante direcciones IP**

| 24. Bitácoras de acceso y operación cotidiana, seguridad aplicable | |
|---|---|
| Soporte físico | El administrador del sistema procura el control y registro conforme a lo siguiente:<br>1. Emite la facultad de accesos a los servidores públicos a fin de que este, en el ejercicio de sus funciones puedan interactuar con una o más vistas del sistema, mediante solicitud escrita.<br>2. La asignación, actualización y remplazo de contraseña que se entrega al personal, se realiza en respuesta a la solicitud escrita mediante sobre cerrado al usuario.<br>3. Las acciones de los autorizados llevan a cabo en el área de resguardo. Para ello, cada una de las personas realiza un vale para realizar cambios dependiendo la acción.<br>4. El administrador del sistema lleva un control de los cambios realizados.<br>5. Se registra en bitácora de eventos ocurridos mediante vale o solicitud de servicios de sistema, fecha de solicitud, área solicitante, clave y nombre del solicitante, nombre de quien autoriza (jefe inmediato), sistema que se reporta, descripción de la solicitud, fecha de terminación del trámite, firma de conformidad del usuario, firma de quien realizo, firma del jefe del departamento. |
| Soporte electrónico | 1. El Responsable del sistema en coordinación con la Subdirección de Tecnologías de la Información lleva un control y registro, conforme a lo siguiente:<br><br>a) Se generan bitácoras de eventos ocurridos a nivel sistema operativo en los equipos (servidores, cortafuegos, almacenamiento masivo) que habilitan la operación del sistema de datos. Entre otras, se generan bitácoras para desempeño del servidor: intentos de acceso (exitosos y fallidos); accesos denegados a usuarios y terminales; uso de herramientas para administración del servidor, y fecha y hora de los eventos anteriores.<br><br>b) Se realiza una bitácora de eventos generados a nivel software aplicativo del sistema de datos personales. Estas bitácoras tienen como registro las actividades de relacionadas con el sistema, si se genera un mensaje de error, acciones de apertura, modificación y cierre de archivos, así como la detención de amenazas de seguridad por parte del software. Cada uno de los eventos configurados en el software quedan registrados. |

**25. Lugar de almacenamiento de las bitácoras y tiempo de conservación y conservación de integridad**

a) Se garantiza copiándolas en un servidor del centro de datos el cual las graba en CD-R.
**Se realiza copia de servidor del centro de datos perteneciente al Instituto Nacional de Pediatría**
b) Algunas se copian cada hora, otras a diario
**Se realiza copia todos los días y se mantiene un respaldo de cada mes y año**
c) La integridad de las copias se garantiza además con "resúmenes" creados por un algoritmo "digestor".
**Por el momento no se cuenta con herramienta de software**
d) Se cuenta con una herramienta de software que automatiza estas operaciones.
**Por el momento no se cuenta con herramienta de software**

Especificarse si las áreas de informática y seguridad de la información han designado una persona que se encarga de realizar un análisis de las bitácoras generadas, conforme a lo siguiente:

Si, el Instituto Nacional de Pediatría actualmente cuenta con personal designado para realizar el análisis de bitácoras

a) Se cuenta con la ayuda de una herramienta informática adquirida para tal propósito. No, se encuentra en proceso

b) Cada semana se llevan a cabo análisis de bitácoras, pero no de todas ellas. Depende de la bitácora y de las amenazas detectadas en el entorno. La bitácora y de las amenazas son detectadas en el entorno.

**26. Registro de incidentes**

Registro de Incidentes en el Sistema Integral De Administración INP (SIA).

1.- Los datos registrados sobre el incidente serán los siguientes:

a) Hora y fecha de incidencia

b) Persona que reporta el incidente

c) Documentación ante incidente (Elaboración de "plan de respuesta a incidente "medidas de seguridad previamente implementadas, identificación de activos, medidas de seguridad de los activos, alertas de seguridad de asociadas a las medidas, propósito de medidas de seguridad para, mitigar el incidente)

d) Registrar si es el incidente es físico o electrónico

e) Documentar como se asegura la integridad de la información mediante el plan de respuesta a incidentes

f) Autorización de recuperación de información por parte del área que reporta

g) Solución del incidente

h) Fecha de conclusión del incidente

Procedimiento en caso de presentarse un incidente.

1. El responsable de seguridad tiene la labor de detectar el incidente
2. El responsable registra y clasifica el incidente del Sistema Integral de Administración (INP).
3. Notifica el incidente al equipo y realiza la revisión de la contención buscando la detección del incidente con el fin de que no se propague y pueda generar más daños a la información o a la arquitectura del SIA
4. El responsable de seguridad genera un informe detallado del incidente a más tardar al día siguiente de lo ocurrido, dicho informe detallará lo ocurrido en el Sistema Integral de Administración (INP).
5. Se documentará el proceso de solución del incidente
6. En caso de pérdida de información de datos personales, el Subdirector de Tecnologías de la Información, al tener conocimiento del incidente de aviso al Director de área para su conocimiento y al titular del área jurídica para presentar denuncia.
7. Después de ocurrir el Incidente se inicia la recuperación, reintegración de activos, monitoreo de nuevas medidas y generación de pruebas de incidente.
8. Posterior a lo ya mencionado se empieza a trabajar sobre la mejora continua, donde se generará documentación final de incidente.

**27. Procedimiento de respaldo y recuperación de datos**

1. Señalar si realiza respaldos completos, diferenciales o incrementales; Completo

2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad; Discos duros, Servidor

3. Cómo y dónde archiva esos medios, Centro de datos y área de Sistemas de la Información

4. Quién es el responsable de realizar estas operaciones (el sujeto obligado o un tercero) El sujeto obligado

**28. Plan de contingencia** Indicar si se cuenta con un plan de contingencia y si este atiende conforme a lo siguiente:)

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.

Este plan de contingencia se encuentra en desarrollo y documentación para el Sistema Integral De Administración INP

1. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia del mismo.

En mención de que se encuentra en desarrollo, una vez establecido se llevarán a cabo las pruebas de eficiencia del mismo.

2. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:

El sistema no cuenta con sitio redundante

a) El tipo de sitio (caliente, tibio o frío);

El Sistema Integral De Administración INP es posible habilitarlo en un sitio frio

b) Si el sitio es propio o subcontratado con un tercero;

| |
|---|
| **Se considera un sitio propio**<br>c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio, y<br>**Se considera equipo y recurso humano institucional**<br>d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.<br>**Es posible habilitarlo en 120 horas.** |

**29. Encargado de datos (**Indicar el Prestador de servicios persona física o moral, pública o privada ajena al INP que sola o conjuntamente con otros, trata datos personales a nombre y por cuenta en subcontratación, conforme a lo siguiente:)

| | | | | |
|---|---|---|---|---|
| Existe un prestador de servicios, persona física o moral, pública o privada ajena al INP que sola o conjuntamente, trate datos personales a nombre y por cuenta de este Instituto | SI | | NO | X |

**30. Plazo de conservación y bloqueo de los datos personales (**periodo en el que la autoridad conservará los datos para efectos de responsabilidades, el cual será equivalente al plazo de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento en términos de la normatividad de aplicable y, cumplido este plazo, deberá procederse a la supresión del dato que implica el borrado físico del mismo, conforme a las siguientes consideraciones:)

a) Deberá considerar lo dispuesto en el Catálogo de disposición documental -un registro general, además, que se debe incluir la siguiente información del Catálogo de disposición documental -un registro general y sistemático que establece los siguientes valores documentales-: (i) los plazos de conservación; (ii) la vigencia documental; (iii) la clasificación de reserva o confidencialidad, y (iv) el destino final de los documentos.

b) Deberá verificar si el mismo tiene valores históricos, científicos, estadísticos o contables. En caso de que contenga dichos valores, los datos personales serán objeto de transferencias secundarias, de conformidad con lo establecido por los catálogos de disposición documenta.

c) Deben atender al valor documental de la información contenida en el mismo, de conformidad con los criterios establecidos por el sujeto obligado en consideración a la posible consulta que de los mismos se requiriera o a cualquier otra implicación jurídica que pudiera existir en razón de la normatividad aplicable.

| 0. SUBDIRECCIÓN DE SERVICIOS GENERALES | Fecha de Elaboración (mes y año): Junio 2024<br>Fecha última Actualización (mes y año): Junio 2024 |
|---|---|
| 1. Nombre del Sistema | Base de datos en Excel de contrataciones del INP |
| 2. Objetivo | Gestión de contrataciones de Servicios y Obra Pública |
| 3. Fundamento Legal | Constitución Política de los Estados Unidos Mexicanos art 134; Ley de Adquisiciones Arrendamientos y Servicios del Sector Público en sus artículos 25, 26, 29 y 45; Reglamento de la Ley de Adquisiciones Arrendamientos y Servicios del Sector Público artículos 35, 39, 48 y 57; Ley de Obras Públicas y Servicios Relacionados con las Mismas en sus artículos 27, 31 y 46; Reglamento de la Ley de Obras Públicas y Servicios Relacionados con las Mismas artículos 34, 36 y 44; Políticas Bases y Lineamientos para la Adquisición, Arrendamientos y Servicios del INP; Políticas Bases y Lineamientos para la contratación de Obras Públicas y Servicios Relacionados con las Mismas en el INP; Estatuto Orgánico del INP en su artículo 48 y demás aplicables a la materia. |

**4. DATOS PERSONALES QUE CONTIENE EL SISTEMA** (Indicar todos los datos personales que son solicitados y que se contienen en el sistema)

✖ **I. Datos de identificación y autentificación** (nombre, domicilio, teléfono fijo y/o celular, correo electrónico personal, estado civil, firma, firma electrónica, cartilla militar, pasaporte lugar y fecha de nacimiento, nacionalidad, edad, fotografía, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), código bidimensional QR idiomas, fotografía), documento de nacionalización, cédula de identificación de extranjeros, acta de nacimiento del titular, actas expedidas por el registro civil, comprobantes de domicilio, nombre de beneficiarios designados,

✖ **II. Datos laborales** (empleos desempeñados, actividades extracurriculares, referencias laborales, referencias personales, recomendaciones, capacitaciones, cursos, idiomas documentos de selección, reclutamiento, nombramiento, incidencias, hojas de servicio, incapacidades, cuidados, gastos médicos mayores, estado cuenta AFORE, expedientes electrónico Único del ISSSTE, cuidados maternos inscripción al ISSSTE, baja del ISSSTE, tramites de jubilación, pensión, actas administrativas, licencias, documento de renuncia, documento de cese. credencial, medidas disciplinarias.

□ **III. Datos de contacto y ubicación** (domicilio, teléfono fijo y/o celular, correo electrónico, redes sociales)

□ **IV. Datos Académicos** (trayectoria académica y formación profesional como son calificaciones, boletas, constancia máxima de estudios, certificados, reconocimientos, títulos, cédulas profesionales)

□ **V. Datos relacionados con intereses personales y profesionales** (pasatiempos, cursos, talleres)

✖ **VI. Datos patrimoniales o financieros** (bienes muebles e inmuebles, ingresos y egresos, cuentas bancarias, seguros, afores, historial crediticio, información fiscal, referencias personales crediticias, póliza de seguro de gastos médicos mayores para extranjeros, número de cuenta bancaria, clave / interbancaria, declaración patrimonial, prestaciones laborales, descuentos, cuotas sindicales, placa, modelo y marca de vehículo, créditos personales, datos de equipo de cómputo propio, marca, modelo, serie, solicitud de potenciación de seguro de vida )

□ **VII. Datos biométricos** (relacionados con las características físicas, fisiológicas, huellas dactilares, los modelos retínales, la estructura facial, voces, geometría de la mano, color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros

□ **VIII. Datos genéticos** (muestras genéticas tejidos o sangre, funciones de ciertos genes, muestras de ADN)

□ **IX. Datos genómicos** (estructura y función del genoma de un organismo, secuencia de moléculas en los genes de un organismo, proteínas, ARN

□ **X. Datos de salud** (estado de salud física o mental, historial clínico, alergias, enfermedades, información relacionada con cuestiones psicológicas o psiquiátricas, incapacidades, intervenciones quirúrgicas, vacunas, certificados o estudios médicos, consumo de sustancias toxicas, uso de aparatos ortopédicos, oftalmológicos, auditivos, prótesis)

□ **XI. Datos ideológicos** (origen racial o étnico; estado de salud pasado, presente y futuro; información genética; creencias religiosas, filosóficas y morales; afiliación sindical; opiniones políticas y preferencia sexual.

☐ XII. **Datos de tránsito o migratorios** (Información sobre nacionalidad y su estadía dentro y fuera de país)

☐ XIII. **Aparatos de asistencia o apoyos funcionales** (de ortesis, prótesis y ayudas técnicas)

☐ XIV. **Datos sobre procedimientos administrativos relativos a una persona que se encuentre sujeta a un procedimiento seguido en forma de juicio.**

☐ En caso de recabar algún dato distinto, favor de indicarlo

_____

**5. FINALIDADES PARA LOS QUE SON TRATADOS LOS DATOS PERSONALES RECABADOS Y SI REQUIERE CONSENTIMIENTO**

Indicar cuales son las finalidades que dan origen y son necesarias para llevar a cabo y mantener la relación jurídica entre el responsable y el titular. las finalidades deben ser concretas, licitas, explicitas y legítimas, relacionada con las atribuciones normativas conferidas.

☐ Integrar el registro de la bolsa de trabajo en línea
☐ Para atender, registrar, dar seguimiento, gestionar y contactarle en relación a la(s) solicitud(es) que realice, para ocupar alguna plaza vacante.
☐ Para integrar registro de los interesados en participar en cursos de capacitación
☐ Para dar cumplimiento y seguimiento a las bases, requisitos y procedimientos para la admisión
☐ Para validar la veracidad y calidad de la información proporcionada por usted.
☐ Para dar continuidad al proceso de admisión.
☐ Para gestionar la aplicación del estudio psicométrico y de admisión que correspondan
☐ Para la aplicación de exámenes de admisión.
☐ Para informarle sobre los resultados de sus exámenes.
☐ Para realizar reportes estadísticos, previa aplicación de un mecanismo de disociación de los datos personales
☐ En caso de existir finalidad distinta, favor de indicarla_____

☐ Gestionar la recepción, expedición y entrega de los documentos físicos y/o digitales que acrediten a la persona interesada.
☐ Para realizar todos los trámites necesarios ante las autoridades correspondientes
☐ Para generar el Formato Único de Movimiento de Personal
☐ Para integrar el expediente de personal en cumplimiento a las disposiciones.
☐ Para identificación, y autentificación como Empleado y/o Servidor Público.
☐ Para generar y administrar credenciales para el acceso a las instalaciones
☐ Para generar los pagos y prestaciones correspondientes
☐ Para realizar trámites de altas, bajas y/o modificaciones ante el ISSSTE
☐ Para la administración del acceso electrónico (contraseñas) a los sistemas, aplicativos e infraestructura tecnológica.
☐ Para preservar la seguridad de las personas usuarias y las instalaciones, durante su ingreso y permanencia en el inmueble
☐ Para la elaboración hojas de servicios
☐ Para el descuento de préstamos, primas de seguro, pensión alimenticia
☐ Para contratación, de los seguros necesarios
☐ Para el cumplimiento de disposiciones fiscales
☐ Para el alta o baja en instituciones de seguridad social.
☐ Para la gestión de una cuenta bancaria que el interesado deberá realizar y comunicar a la cual se transfiera el pago de sueldos, salarios y prestaciones, en su caso.
☐ Para la integración de información relacionada con el estado de salud, incapacidades y licencias
☐ Para el otorgamiento de becas, premios, estímulos o recompensas.
☐ Para gestiones relacionados con procesos de certificación
☐ Para monitoreo en las cámaras de seguridad, circuito cerrado y grabaciones, así como para registro de asistencia
☐ Para evidenciar la organización de eventos compartiendo imágenes y fotografías
☐ Para realizar gestiones de los prestadores de Servicio Social y Prácticas Profesionales
☐ Para la celebración de instrumentos jurídicos en materia laboral
☐ Para efectos de control, auditoria y fiscalización que deriven de la relación laboral
☐ Para evaluar su desempeño
☐ Para comunicar la implementación de políticas y programas
☐ En caso de solicitarlo, para inscribirle y participar en cursos, talleres, programas y cualquier tipo de evento
☐ Para la emisión de constancias y demás reconocimientos correspondientes.
☐ Para contactar a sus familiares o terceros señalados como contacto en caso de una emergencia
☐ Para tramites de facturación

Para realizar estudios de mercado en el caso de procedimientos de contratación que así lo requieran
☒ Para integración de expedientes de propuestas legal, técnica y económica en procesos de contratación, concesión, contratos, convenios, permisos, licencias o autorizaciones otorgados, procedimientos de adjudicación directa, invitación restringida y licitación de cualquier naturaleza, según sea el caso
☒ Para la elaboración de actas derivadas de procedimiento de contratación aplicable
☒ Para la elaboración de contratos en caso de ser adjudicado
☒ Para integrar y actualizar directorio de contratistas en caso de personas físicas
☒ Para atender requerimientos de autoridad
☐ Para realizar reportes estadísticos previa aplicación de un mecanismo de disociación de los datos personales.
☐ Para informarle de alguna vacante
☐ Para informarme sobre futuros eventos realizados por el Instituto o en colaboración.
☐ Para llevar el registro de asistencia en el caso de cursos de capacitación
☐ Para aquellos eventos, capacitaciones o pláticas informativas que impliquen el uso de plataforma de videoconferencia o diversos medios electrónicos, se grabarán las sesiones, a fin de documentar las sesiones como evidencia de su realización, quedando documentada la imagen y registro de voz de las y los participantes de esta
☐ Para conocer las necesidades de capacitación
☐ En caso de existir finalidad distinta, favor de indicarla _____

| Requiere consentimiento | Supuesto artículo 22, que se actualiza en su caso | Tipo de consentimiento |
|---|---|---|
| ☐ Si<br>☒ No | Artículo 22. El responsable no estará obligado a recabar el consentimiento del titular para el tratamiento de sus datos personales en los siguientes casos:<br>☒ I. Cuando una ley así lo disponga, debiendo dichos supuestos ser acordes con las bases, principios y disposiciones establecidos en esta Ley, en ningún caso, podrán contravenirla;<br>☐ II. Cuando las transferencias que se realicen entre responsables, sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;<br>☐ III. Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;<br>☐ IV. Para el reconocimiento o defensa de derechos del titular ante autoridad competente;<br>☒ V. Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;<br>☐ VI. Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;<br>☐ VII. Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico, la prestación de asistencia sanitaria; | ☒ Tácito<br>☐ Expreso<br>☐ Expreso por escrito |

| | | |
|---|---|---|
| | ☐ VIII. Cuando los datos personales figuren en fuentes de acceso público<br>☐ IX. Cuando los datos personales se sometan a un procedimiento previo de disociación, o<br>☐ X. Cuando el titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley en la materia. | |

**6.FORMA DE OBTENCIÓN DE LOS DATOS PERSONALES** (Indicar la forma en que se obtienen los datos personales que obran en el Sistema o bien si estos provienen de otro Sistema)

| | | |
|---|---|---|
| ✖ Gráfico<br>✖ Electrónico<br>☐ Telefónico<br>☐ Audiovisual<br>☐ Óptico<br>☐ Sonoro<br>☐ En caso de existir otro medio no enlistado, favor de indicar cual<br>_____ | **Directa** ✖ | **Indirecta** (obtenida, creada, generada en algún otro sistema) ☐<br>**Señalar cual:** |

**7. Responsable del Sistema** Se entiende a la persona Titular del Área Responsable propietaria del Sistema

| | |
|---|---|
| Nombre | Ricardo Castro Diaz |
| Cargo | Subdirector de Servicios Generales |
| Área de adscripción | Servicios Generales |
| Teléfono | 55 1084 0900 Ext 1173. |
| Correo electrónico | rcastrod@pediatria.gob.mx |
| Función | Supervisión de contratos, convenios sobre servicios y obra pública |
| Obligación | Supervisión de contratos, convenios sobre servicios y obra pública |

**8. Encargado.** La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras **tratara** datos personales a nombre y cuenta del responsable.

| | |
|---|---|
| Nombre | |
| Cargo | |
| Área de adscripción | |
| Teléfono | |
| Correo electrónico | |
| Función | |
| Obligación | |

**9. Propietario del Sistema** La persona que **genera** la información y decide sobre cómo se realiza el tratamiento de los datos personales que tiene asignados, conforme a facultades y atribuciones previstas en el Estatuto Orgánico del Instituto.

| | |
|---|---|
| Nombre | |
| Cargo | |
| Área de adscripción | |
| Teléfono | |
| Correo electrónico | |
| Función | |
| Obligación | |

**10. Administrador** La persona responsable de **otorgar** permisos y vigilar la ejecución de actividades asignadas a los usuarios genéricos.

| | |
|---|---|
| Nombre | |
| Cargo | |
| Área de adscripción | |
| Teléfono | |
| Correo electrónico | |
| Función | |
| Obligación | |

**11. Custodio** La persona que se **encarga** de la gestión de activos informáticos, su administración diaria y el monitoreo de la seguridad en los sistemas de tratamiento de datos personales que se encuentran bajo su resguardo.

| | |
|---|---|
| Nombre | Ing. Misael Teófilo Tovar Cruz |
| Cargo | Subdirector de Tecnologías de la Información |
| Área de adscripción | Dirección de Planeación Grafico **Directa** |
| Teléfono | 55 1084 0900 Ext 1495 |
| Correo electrónico | mtovarc@pediatria.gob.mx |
| Función | Implementar medidas de seguridad informática, gestionar incidentes, promover la conciencia de seguridad de la información. Mantener en la medida de lo posible la protección adecuada de los datos de los sistemas informáticos. |
| Obligación | Mantener en optimo funcionamiento el hardware donde se registran los datos |
| **12. Usuario Genérico** La persona que **utiliza** el sistema de tratamiento de datos personales para interactuar con la información y realizar sus actividades, atendiendo a las medidas de seguridad, así como a la Confidencialidad, Integridad y Disponibilidad de la Información | |
| Nombre | Diana Ivonne Guerra Quiroz |
| Cargo | Apoyo Administrativo |
| Área de adscripción | Departamento de Conservación y Mantenimiento |
| Teléfono | 55 10 84 09 00 ext. 1385 |
| Correo electrónico | eguerraq@pediatria.gob.mx |
| Función | Registrar los contratos en la base de datos |
| Obligación | Registro |
| Nivel 2 Subdirección | |
| | |
| Nombre | Andrea Espinosa Gutiérrez |
| Cargo | Apoyo Administrativo |
| Área de adscripción | Departamento de Conservación y Mantenimiento |
| Teléfono | 55 10 84 09 00 ext. 1385 |
| Correo electrónico | aespinosag@pediatria.gob.mx |
| Función | Registrar los contratos en la base de datos |
| Obligación | Registro |
| | |
| Nombre | Cristian Iván Flores Chávez |
| Cargo | Soporte Administrativo |
| Área de adscripción | Departamento de Conservación y Mantenimiento |
| Teléfono | 55 10 84 09 00 ext. 1385 |
| Correo electrónico | cfloresc@pediatria.gob.mx |
| Función | Registrar los contratos en la base de datos |
| Obligación | Registro |
| | |
| Nombre | Juan Enrique Martínez Jiménez |
| Cargo | Apoyo Administrativo |
| Área de adscripción | Departamento de Conservación y Mantenimiento |
| Teléfono | 55 10 84 09 00 ext. 1385 |
| Correo electrónico | jmartinezj@pediatria.gob.mx |
| Función | Registrar los contratos en la base de datos |
| Obligación | Registro |
| | |
| Nombre | Luis Fernando Rios Morales |
| Cargo | Administrativo |
| Área de adscripción | Subdirección de Servicios Generales |
| Teléfono | 55 10 84 09 00 ext. 1173 |
| Correo electrónico | lriosm@pediatria.gob.mx |
| Función | Registrar los contratos en la base de datos |
| Obligación | Registro |
| | |
| Nombre | Edgar Ruiz Gómez |
| Cargo | Administrativo |
| Área de adscripción | Subdirección de Servicios Generales |
| Teléfono | 55 10 84 09 00 ext. 1173 |
| Correo electrónico | |
| Función | Registrar los contratos en la base de datos |

| | |
|---|---|
| Obligación | Registro |
| | |
| Nombre | Jocelyn Huerta Nava |
| Cargo | Apoyo Administrativo |
| Área de adscripción | Departamento de Servicios de Apoyo |
| Teléfono | 55 10 84 09 00 ext. 1181 |
| Correo electrónico | |
| Función | Registrar los contratos en la base de datos |
| Obligación | Registro |
| | |
| | |

**13. Tipo de soporte de la base de datos y donde se ubica el mismo** (Deberá indicar las características del lugar donde se resguardan los soportes, se deberá otorgar información conforme lo siguiente:

a) **Para soportes físicos**, el sujeto obligado deberá incluir una descripción escrita con detalles sobre las características físicas de la oficina, almacén o bodega donde resguarda dichos soportes;

b) **Para soportes electrónicos**, la descripción ofrecida por el sujeto obligado deberá incluir un diagrama de la arquitectura de seguridad en el cual sea posible apreciar el flujo de datos a través de la o las redes electrónicas que interconectan los equipos (clientes, servidores, cortafuegos, unidades de almacenamiento, entre otros) del sistema. Además, deberá describir las medidas de seguridad física que ha implementado para la protección del centro de datos donde residen tales soportes, y

c) **En caso de que el sistema ocupe ambos tipos de soportes**, deberá presentar las descripciones correspondientes a cada uno, en términos de lo señalado en los incisos a) y b) anteriores)

☐ g) Físico _____

☐ h) Electrónico

✖ i) Ambos La información de los contratos se registra en una base de datos en Excel en los equipos de cómputo de los usuarios y en físico en carpetas.

**14. Realiza transferencias de datos personales** (Entiéndase como la comunicación de datos o entrega total o parcial de los mismos, a cualquier persona distinta a su titular, sea mediante el uso de medios físicos o electrónicos, tales como la interconexión de computadoras o bases de datos, acceso a redes de telecomunicación, así como a través de la utilización de cualquier otra tecnología que lo permita. En el ámbito de la Administración Pública Federal se tienen)

☐ SI ✖ NO

*Describir en que consiste la transferencia conforme a lo siguiente:

☐ 7. Interinstitucionales (Transmisiones de datos a dependencias y entidades de la APF. Entidades federativas y municipios)
☐ 8. Internacionales (Transmisiones gobiernos u organismos internacionales)
☐ 9. Con entes privados u organizaciones civiles públicas o privadas

| ¿Qué datos personales o categorías son transferidos? | ¿A quién son transferidos? | ¿Para qué finalidad son transferidos? |
|---|---|---|
| | | |

**Se requiere consentimiento**

SI ☐ NO ☐

| Supuestos artículos 22, 66 ó 70 que se actualizan en su caso | Tipo de consentimiento que se requiere para la transferencia | La transferencia requiere la suscripción de clausulas contractuales, convenios de colaboración u otro instrumento jurídico. |
|---|---|---|
| | ☐ Tácito | |

| | | |
|---|---|---|
| | ☐ Expreso por escrito | ☐ SI ☐ NO |

**15. Portabilidad de datos** (Indicar si las características del sistema permiten apreciar un sistema de datos personales estructurado comúnmente utilizado.)

| | |
|---|---|
| SI ✖ | NO ☐ |

**16. Difusión de datos personales** (Indicar si en el tratamiento se realiza la difusión de datos personales y su fundamentación)

SI ✖ Fundamento SIPOT Art 70 Fracc 28

NO ☐

**17. Nivel de protección que requieren los datos** (indicar el nivel aplicable, el cual estará determinado en base a los datos en posesión, siguiendo los criterios internacionales de seguridad para el resguardo eficaz de los mismos. Los niveles de seguridad responden a la mayor o menor necesidad de garantizar la integridad de los datos personales, conforme a lo siguiente)

✖ C. **Nivel Básico. – I** Datos de identificación y autentificación, **II** Datos laborales, **III** Datos de contacto, **V.** Datos relacionados con intereses personales y profesionales

☐ D. **Nivel Medio. - IV.** Datos académicos, **VI.** Datos patrimoniales o financieros, **XII**. Datos de tránsito o migratorios, **XIII.** Aparatos de asistencia o apoyos funcionales, **XIV.** Datos sobre procedimientos administrativos seguido en forma de juicio

☐ C. **Nivel Alto. - VII.** Datos biométricos, **VIII**. Datos genéticos, **IX.** Datos genómicos, **X.** Datos de salud,**XI.** Datos ideológicos

**18. Actualización de la información contenida en el sistema (**indicar la frecuencia con que se actualiza la información directamente en la base de datos del sistema)

☐ Diaria ☐ Bimestral Trimestral ☐ Semestral ☐ Anual ✖ Otra especificar Mensual

**19. Plazo de conservación de los datos personales** (indicar cuanto tiempo permanecerán los datos personales en el Sistema de Datos conforme a su vigencia y finalidad, es decir atendiendo al ciclo de vida del trámite o servicio por motivo del cual se obtuvieron, basado en los instrumentos de control archivístico, CADIDO y Cuadro General de Clasificación Archivística)

✖ 6 años ☐ _____ meses ☐ _____ días Otro especificar_____

| Indicar Sección de archivos | Serie de archivo | Subserie de archivo en su caso |
|---|---|---|
| 7C | 7C.1 | |

**20. Medidas de Seguridad** (indicar los elementos de seguridad con que se cuenta y se abordan en tres modalidades tomando como base el estándar internacional ISO/IEC 27002:2005 que se refiere a mejores prácticas sobre seguridad de la información)

| | |
|---|---|
| Físicas | ✖ Portación de credencial institucional<br>✖ Acceso solo a áreas autorizadas<br>☐ Acceso a instalaciones con código numérico o de barras<br>☐ Acceso a instalaciones en base a dato biométrico<br>☐ Puertas con cerradura, cerrojos, chapas. etc<br>✖ Control e identificación de equipos portátiles de usuarios<br>☐ Control e identificación de equipos portátiles de empleados trabajadores<br>☐ Control de llaves<br>☐ Control de apertura y cierre de puertas externas e internas<br>Otro especificar_____ |
| Administrativas | ✖ **Política de seguridad.**: Código de Conducta, Código de Ética y Política general de Seguridad de la Información |

✖

| | |
|---|---|
| | Cumplimiento de la normatividad. Contrato de servicios y Acuerdo de confidencialidad<br><br>✖**Organización de la seguridad de la información.** Política de Seguridad de la información (Garantizar la confidencialidad, integridad y disponibilidad de la información del INP, a partir del establecimiento de lineamientos, políticas, controles, procedimientos y el fomento de una cultura de seguridad de la información.)<br><br>✖ **Seguridad relacionada a los recursos humanos.** Política De Recursos Humanos (Establecer los lineamientos, en materia de seguridad de la información, sobre el proceso de Recursos Humanos que deben pasar previo a la relación laboral, durante la relación laboral con el Instituto Nacional de Pediatría y una vez que se dé por terminada la relación laboral.)<br><br>✖ **Administración de incidentes.** Plan De Contingencia (Se establece el procedimiento de responsabilidades para la detección, escalado y mitigación de incidentes de seguridad de la información del sistema través de la Subdirección de TI).<br><br>✖**Continuidad de las operaciones.** Política de Gestión (Establecer los lineamientos, en materia de seguridad de la información, para identificar, detectar, registrar, reportar y atender de forma adecuada y eficaz los incidentes de seguridad de la información con la finalidad de reducir el posible impacto de estos en las operaciones del INP.) Teniendo en cuenta el equipo de protección civil ante desastres naturales |
| Técnicas | ✖**Gestión de comunicaciones y operaciones**. Política de tecnologías Móviles (Establece lineamientos, en materia de seguridad de la información, para prevenir pérdidas, daños, hurtos o el compromiso de los recursos tecnológicos, así como para la seguridad y protección de los equipos de escritorio y portátiles contra amenazas físicas y lógicas.), uso de perfiles de usuario y software antivirus<br><br>✖**Control de acceso**.<br>Política de administración de la seguridad de la red (Establece los lineamientos, en materia de seguridad de la información, sobre la administración de seguridad de la red y el acceso y restricción a las redes del INP, que permitan asegurar la confidencialidad, integridad y disponibilidad de la información que se transmite a través de estas), Directorio Activo, Perfiles de usuarios en sistemas informáticos<br><br>✖**Adquisición, desarrollo, uso y mantenimiento de sistemas de información**: Política de Sistemas, Aplicaciones y Servicios (Establece los lineamientos, en materia de seguridad de la información, para mantener la seguridad de la información durante la adquisición, desarrollo y mantenimiento de sistemas, así como establecer lineamientos a seguir por parte de los colaboradores del Instituto Nacional de Pediatría, para asegurar la integración de la seguridad de la información en los sistemas de información actuales y futuros que sean parte del INP.) |
| **21. Acceso a instalaciones** | |
| 1. **Seguridad perimetral exterior**<br>¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones?<br>Controles biométricos y portación de credencial<br>• **Personal que labora en el Instituto Nacional de Pediatría (INP)**<br>**Control de acceso biométrico de reconocimiento facial para el personal, portación de credencial Institucional, circuito cerrado de Televisión y personal de vigilancia que se idéntica visualmente con su uniforme**<br>• **Personal Externo al INP**<br>**Se cuenta con registro en ventanilla con el personal de vigilancia, se capturan sus datos y fotografía de la persona a ingresar y se comparte un código de tipo quick response que lo deben de portar durante su visita**<br>• **Registro de familiares del paciente**<br>**Se hace mediante el carnet del paciente**<br>¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones?<br>a) ¿Cómo las identifica? **El personal porta la credencial dentro de la institución,**<br>b) ¿Cómo las autentifica? **Con la inspección visual y monitoreo en el circuito cerrado**<br>c) ¿Cómo les autoriza el acceso? **Por medio del personal de seguridad cuando se porta la credencial**<br><br>2. **Seguridad perimetral interior**: | |

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? **Se ingresa a partir de una puerta con control biométrico de huella dactilar al centro de datos principal y registro de bitácora, puertas con acceso restringido a los cuartos de comunicación secundarios**
Para las personas que acceden a dichos espacios interiores:
a) ¿Cómo las identifica? **El personal tiene la obligación de portar la credencial en todo momento, huella dactilar en el centro de datos y monitoreo mediante circuito cerrado**
b) ¿Cómo las autentifica? Existen perfiles de acceso al centro de datos por el reconocimiento dactilar, **Se cuenta con circuito cerrado en el hospital**
c) ¿Cómo les autoriza el acceso? **Se asigna al personal del Instituto, registra su entrada con biométrico en el centro de datos, existe una bitácora de acceso y se registra hora, nombre del personal que ingresa, hora de entrada, hora de salida y motivo del ingreso.**

**22. Perfiles de usuario y contraseña**

1. Modelo de control de acceso:
a) ¿Es obligatorio? **Si**
b) ¿Es discrecional? **Si**
c) ¿Está basado en roles (perfiles) o grupos? **Si**
d) ¿Está basado en reglas? **Sí**

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
a) ¿Cuenta con un sistema operativo de red instalado en sus equipos? **Sí**
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas? **Sí**
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? **Solo las contraseñas**

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de datos personales:
a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas? **No**
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? **No**

4. Administración de perfiles de usuario y contraseñas:
a) ¿Quién da de alta nuevos perfiles? **Administradores (Encargados) del área**
b) ¿Quién autoriza la creación de nuevos perfiles? **Jefe Inmediato del Área**
c) ¿Se lleva registro de la creación de nuevos perfiles? **No**

5. Acceso remoto al sistema de datos personales:
a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? **No**
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? **No**
c) ¿Cómo se evita el acceso remoto no autorizado? **Por restricción de acceso mediante direcciones IP**

**23. Bitácoras de acceso y operación cotidiana, seguridad aplicable**

| | |
|---|---|
| Soporte físico | **El responsable del área procura el control y registro conforme a lo siguiente:**<br><br>6. **Emite la facultad de accesos a los servidores públicos a fin de que este, en el ejercicio de sus funciones puedan interactuar con el equipo de cómputo para el registro de los datos**<br>7. **La asignación, actualización y remplazo de contraseña que se entrega al personal para el uso del equipo de cómputo, se realiza en respuesta a la solicitud del responsable del área y se llena el formato de asignación de equipo de cómputo.**<br>8. **Los perfiles del usuario es asignado conforme a los creados en el Directorio Activo.**<br><br>**Las incidencias son registras mediante la solicitud de servicios en la que se detalla, fecha de solicitud, área solicitante, clave y nombre del solicitante, nombre de quien autoriza (jefe inmediato), sistema que se reporta, descripción de la solicitud, fecha de terminación del trámite, firma de conformidad del usuario, firma de quien realizo** |
| Soporte electrónico | **1. El Responsable del área en coordinación con la Subdirección de Tecnologías de la Información lleva un control y registro, conforme a lo siguiente:** |

| | |
|---|---|
| | Control de acceso al equipo de cómputo mediante Directorio Activo |

**24. Lugar de almacenamiento de las bitácoras y tiempo de conservación y conservación de integridad:**

a) **Se realiza copia en un sistema de almacenamiento en el centro de datos perteneciente al Instituto Nacional de Pediatría**
b) **Se realiza copia todos los días durante una semana y se mantiene un respaldo de cuatro semanas, al termino del mes y año**
c) **Se realiza restauración de bases de datos para verificar su confiablidad**

Especificarse si las áreas de informática y seguridad de la información han designado una persona que se encarga de realizar un análisis de las bitácoras generadas, conforme a lo siguiente:
**Si, el Instituto Nacional de Pediatría actualmente cuenta con personal designado para realizar el análisis de bitácoras**
a) Se cuenta con la ayuda de una herramienta informática adquirida para tal propósito. **No, se realiza de manera manual**
b) Cada semana se llevan a cabo análisis de bitácoras, pero no de todas ellas. Depende de la bitácora y de las amenazas detectadas en el entorno. **La bitácora y de las amenazas son detectadas en el entorno.**

**25. Registro de incidentes**

1 **Registro de Incidentes en el Los equipos de cómputo**
**1.- Los datos registrados sobre el incidente serán los siguientes:**

i) **Hora y fecha de incidencia**
j) **Persona que reporta el incidente**
k) **Plan de respuesta a incidentes**
l) **Documentación ante incidente (Tipo de incidente, Efectos del incidente, identificación de activos, medidas de seguridad de los activos, de ser necesario, establecimiento de nuevos controles, mitigar el incidente)**
m) **Autorización de recuperación de información por parte del área que reporta**
n) **Solución del incidente**
o) **Fecha de conclusión del incidente**

**Procedimiento en caso de presentarse un incidente.**

9. **El responsable de seguridad de la información tiene la labor de detectar el incidente**
10. **El responsable registra y clasifica el incidente de los datos y/o información reportada**
11. **Notifica el incidente al equipo y realiza la revisión de la contención buscando la detección del incidente con el fin de que no se propague y pueda generar más daños a la información**
12. **El responsable de seguridad genera un informe detallado del incidente a más tardar al día siguiente de lo ocurrido, dicho informe detallará lo ocurrido**
13. **Se documentará el proceso de solución del incidente**
14. **En caso de pérdida de información de datos personales, el Subdirector de Tecnologías de la Información, al tener conocimiento del incidente de aviso al Director de área para su conocimiento y al titular del área jurídica para presentar denuncia.**
15. **Después de ocurrir el Incidente se inicia la recuperación, reintegración de activos, monitoreo de nuevas medidas y generación de pruebas de incidente.**
16. **Posterior a lo ya mencionado se empieza a trabajar sobre la mejora continua, donde se generará documentación final de incidente.**

**26. Procedimiento de respaldo y recuperación de datos** :

11. Señalar si realiza respaldos completos, diferenciales o incrementales; **Los respaldos se coordinan por el responsable del área de manera completa**
2. El tipo de medios que utiliza para almacenar las copias de seguridad; **Discos duros**
3. Cómo y dónde archiva esos medios, **Oficina del responsable del área**
4. Quién es el responsable de realizar estas operaciones **El sujeto obligado**

**27. Plan de contingencia** Indicar si se cuenta con un plan de contingencia y si este atiende conforme a lo siguiente:)

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.

**Este plan de contingencia se encuentra en desarrollo y documentación**

**28. Encargado de datos (**Indicar el Prestador de servicios persona física o moral, pública o privada ajena al INP que sola o conjuntamente con otros, trata datos personales a nombre y por cuenta en subcontratación, conforme a lo siguiente:)

| | | | | |
|---|---|---|---|---|
| Existe un prestador de servicios, persona física o moral, pública o privada ajena al INP que sola o conjuntamente, trate datos personales a nombre y por cuenta de este Instituto | SI | | NO | X |

**29. Plazo de conservación y bloqueo de los datos personales (**periodo en el que la autoridad conservará los datos para efectos de responsabilidades, el cual será equivalente al plazo de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento en términos de la normatividad de aplicable y, cumplido este plazo, deberá procederse a la supresión del dato que implica el borrado físico del mismo, conforme a las siguientes consideraciones:)

a) Deberá considerar lo dispuesto en el Catálogo de disposición documental -un registro general, además, que se debe incluir la siguiente información del Catálogo de disposición documental -un registro general y sistemático que establece los siguientes valores documentales-: (i) los plazos de conservación; (ii) la vigencia documental; (iii) la clasificación de reserva o confidencialidad, y (iv) el destino final de los documentos.

b) Deberá verificar si el mismo tiene valores históricos, científicos, estadísticos o contables. En caso de que contenga dichos valores, los datos personales serán objeto de transferencias secundarias, de conformidad con lo establecido por los catálogos de disposición documenta.

c) Deben atender al valor documental de la información contenida en el mismo, de conformidad con los criterios establecidos por el sujeto obligado en consideración a la posible consulta que de los mismos se requiriera o a cualquier otra implicación jurídica que pudiera existir en razón de la normatividad aplicable.

| 0. Subdirección de Finanzas | Fecha de Elaboración (mes y año): Junio 2024<br>Fecha última Actualización (mes y año): Junio 2024 |
|---|---|
| 1. Nombre del Sistema | Sistema de gestión para las operaciones financieras y presupuestales del INP |
| 2. Objetivo | Gestionar las operaciones financieras y presupuestales del INP. |
| 3. Fundamento Legal | Indicar el fundamento legal que faculta al responsable para llevar a cabo el tratamiento, indicando los artículos, apartados, fracciones, incisos y nombre de los ordenamientos o disposición normativa vigente que le confiere atribuciones para realizar el tratamiento de datos personales, precisando su fecha de publicación o, en su caso, de la última reforma o modificación. |

**4. DATOS PERSONALES QUE CONTIENE EL SISTEMA (**Indicar todos los datos personales que son solicitados y que se contienen en el sistema)

☒ **I. Datos de identificación y autentificación** (nombre, domicilio, teléfono fijo y/o celular, correo electrónico personal, estado civil, firma, firma electrónica, cartilla militar, pasaporte lugar y fecha de nacimiento, nacionalidad, edad, fotografía, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), código bidimensional QR idiomas, fotografía), documento de nacionalización, cédula de identificación de extranjeros, acta de nacimiento del titular, actas expedidas por el registro civil, comprobantes de domicilio, nombre de beneficiarios designados,

☐ **II. Datos laborales** (empleos desempeñados, actividades extracurriculares, referencias laborales, referencias personales, recomendaciones, capacitaciones, cursos, idiomas documentos de selección, reclutamiento, nombramiento, incidencias, hojas de servicio, incapacidades, cuidados, gastos médicos mayores, estado cuenta AFORE, expedientes electrónico Único del ISSSTE, cuidados maternos inscripción al ISSSTE, baja del ISSSTE, tramites de jubilación, pensión, actas administrativas, licencias, documento de renuncia, documento de cese. credencial, medidas disciplinarias.

☐ **III. Datos de contacto y ubicación** (domicilio, teléfono fijo y/o celular, correo electrónico, redes sociales)

☐ **IV. Datos Académicos** (trayectoria académica y formación profesional como son calificaciones, boletas, constancia máxima de estudios, certificados, reconocimientos, títulos, cédulas profesionales)

☐ **V. Datos relacionados con intereses personales y profesionales** (pasatiempos, cursos, talleres)

☒ **VI. Datos patrimoniales o financieros** (bienes muebles e inmuebles, ingresos y egresos, cuentas bancarias, seguros, afores, historial crediticio, información fiscal, referencias personales crediticias, póliza de seguro de gastos médicos mayores para extranjeros, número de cuenta bancaria, clave / interbancaria, declaración patrimonial, prestaciones laborales, descuentos, cuotas sindicales, placa, modelo y marca de vehículo, créditos personales, datos de equipo de cómputo propio, marca, modelo, serie, solicitud de potenciación de seguro de vida )

☐ **VII. Datos biométricos** (relacionados con las características físicas, fisiológicas, huellas dactilares, los modelos retínales, la estructura facial, voces, geometría de la mano, color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros

☐ **VIII. Datos genéticos** (muestras genéticas tejidos o sangre, funciones de ciertos genes, muestras de ADN)

☐ **IX. Datos genómicos** (estructura y función del genoma de un organismo, secuencia de moléculas en los genes de un organismo, proteínas, ARN

☐ **X. Datos de salud** (estado de salud física o mental, historial clínico, alergias, enfermedades, información relacionada con cuestiones psicológicas o psiquiátricas, incapacidades, intervenciones quirúrgicas, vacunas, certificados o estudios médicos, consumo de sustancias toxicas, uso de aparatos ortopédicos, oftalmológicos, auditivos, prótesis)

☐ **XI. Datos ideológicos** (origen racial o étnico; estado de salud pasado, presente y futuro; información genética; creencias religiosas, filosóficas y morales; afiliación sindical; opiniones políticas y preferencia sexual.

☐ **XII. Datos de tránsito o migratorios** (Información sobre nacionalidad y su estadía dentro y fuera de país)

☐ **XIII. Aparatos de asistencia o apoyos funcionales** (de ortesis, prótesis y ayudas técnicas)

☐ XIV. **Datos sobre procedimientos administrativos relativos a una persona que se encuentre sujeta a un procedimiento seguido en forma de juicio.**

☐ En caso de recabar algún dato distinto, favor de indicarlo

_____

**5. FINALIDADES PARA LOS QUE SON TRATADOS LOS DATOS PERSONALES RECABADOS Y SI REQUIERE CONSENTIMIENTO**

Indicar cuales son las finalidades que dan origen y son necesarias para llevar a cabo y mantener la relación jurídica entre el responsable y el titular. las finalidades deben ser concretas, licitas, explicitas y legítimas, relacionada con las atribuciones normativas conferidas.

☐ Integrar el registro de la bolsa de trabajo en línea
☐ Para atender, registrar, dar seguimiento, gestionar y contactarle en relación a la(s) solicitud(es) que realice, para ocupar alguna plaza vacante.
☐ Para integrar registro de los interesados en participar en cursos de capacitación
☐ Para dar cumplimiento y seguimiento a las bases, requisitos y procedimientos para la admisión
☐ Para validar la veracidad y calidad de la información proporcionada por usted.
☐ Para dar continuidad al proceso de admisión.
☐ Para gestionar la aplicación del estudio psicométrico y de admisión que correspondan
☐ Para la aplicación de exámenes de admisión.
☐ Para informarle sobre los resultados de sus exámenes.
☐ Para realizar reportes estadísticos, previa aplicación de un mecanismo de disociación de los datos personales
☐ En caso de existir finalidad distinta, favor de indicarla_____

☐ Gestionar la recepción, expedición y entrega de los documentos físicos y/o digitales que acrediten a la persona interesada.
☐ Para realizar todos los trámites necesarios ante las autoridades correspondientes
☐ Para generar el Formato Único de Movimiento de Personal
☐ Para integrar el expediente de personal en cumplimiento a las disposiciones.
☐ Para identificación, y autentificación como Empleado y/o Servidor Público.
☐ Para generar y administrar credenciales para el acceso a las instalaciones
☐ Para generar los pagos y prestaciones correspondientes
☐ Para realizar trámites de altas, bajas y/o modificaciones ante el ISSSTE
☐ Para la administración del acceso electrónico (contraseñas) a los sistemas, aplicativos e infraestructura tecnológica.
☐ Para preservar la seguridad de las personas usuarias y las instalaciones, durante su ingreso y permanencia en el inmueble
☐ Para la elaboración hojas de servicios
☐ Para el descuento de préstamos, primas de seguro, pensión alimenticia
☐ Para contratación, de los seguros necesarios
☐ Para el cumplimiento de disposiciones fiscales
☐ Para el alta o baja en instituciones de seguridad social.
☐ Para la gestión de una cuenta bancaria que el interesado deberá realizar y comunicar a la cual se transfiera el pago de sueldos, salarios y prestaciones, en su caso.
☐ Para la integración de información relacionada con el estado de salud, incapacidades y licencias
☐ Para el otorgamiento de becas, premios, estímulos o recompensas.
☐ Para gestiones relacionados con procesos de certificación
☐ Para monitoreo en las cámaras de seguridad, circuito cerrado y grabaciones, así como para registro de asistencia
☐ Para evidenciar la organización de eventos compartiendo imágenes y fotografías
☐ Para realizar gestiones de los prestadores de Servicio Social y Prácticas Profesionales
☐ Para la celebración de instrumentos jurídicos en materia laboral
☒ Para efectos de control, auditoria y fiscalizaciones financieras
☐ Para evaluar su desempeño
☐ Para comunicar la implementación de políticas y programas
☐ En caso de solicitarlo, para inscribirle y participar en cursos, talleres, programas y cualquier tipo de evento
☐ Para la emisión de constancias y demás reconocimientos correspondientes.
☐ Para contactar a sus familiares o terceros señalados como contacto en caso de una emergencia
☒ Para tramites de facturación
☐ Para realizar estudios de mercado en el caso de procedimientos de contratación que así lo requieran

- ☐ Para integración de expedientes de propuestas legal, técnica y económica en procesos de contratación, concesión, contratos, convenios, permisos, licencias o autorizaciones otorgados, procedimientos de adjudicación directa, invitación restringida y licitación de cualquier naturaleza, según sea el caso
- ■ Para la elaboración de actas derivadas de procedimiento de contratación aplicable
- ☐ Para la elaboración de contratos en caso de ser adjudicado
- ☐ Para integrar y actualizar directorio de contratistas en caso de personas físicas
- ☐ Para atender requerimientos de autoridad
- ☐ Para realizar reportes estadísticos previa aplicación de un mecanismo de disociación de los datos personales.
- ☐ Para informarle de alguna vacante
- ☐ Para informarme sobre futuros eventos realizados por el Instituto o en colaboración.
- ☐ Para llevar el registro de asistencia en el caso de cursos de capacitación
- ☐ Para aquellos eventos, capacitaciones o pláticas informativas que impliquen el uso de plataforma de videoconferencia o diversos medios electrónicos, se grabarán las sesiones, a fin de documentar las sesiones como evidencia de su realización, quedando documentada la imagen y registro de voz de las y los participantes de esta
- ☐ Para conocer las necesidades de capacitación
- ☐ En caso de existir finalidad distinta, favor de indicarla _____

| Requiere consentimiento | Supuesto artículo 22, que se actualiza en su caso | Tipo de consentimiento |
|---|---|---|
| ☐ Si<br>☒ No | Artículo 22. El responsable no estará obligado a recabar el consentimiento del titular para el tratamiento de sus datos personales en los siguientes casos:<br>☒ I. Cuando una ley así lo disponga, debiendo dichos supuestos ser acordes con las bases, principios y disposiciones establecidos en esta Ley, en ningún caso, podrán contravenirla;<br>☐ II. Cuando las transferencias que se realicen entre responsables, sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;<br>☐ III. Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;<br>☐ IV. Para el reconocimiento o defensa de derechos del titular ante autoridad competente;<br>☒ V. Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;<br>☐ VI. Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;<br>☐ VII. Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico, la prestación de asistencia sanitaria;<br>☐ VIII. Cuando los datos personales figuren en fuentes de acceso público | ☒ Tácito<br>☐ Expreso<br>☐ Expreso por escrito |

| | | |
|---|---|---|
| | ☐ IX. Cuando los datos personales se sometan a un procedimiento previo de disociación, o<br>☐ X. Cuando el titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley en la materia | |

| **6.FORMA DE OBTENCIÓN DE LOS DATOS PERSONALES** (Indicar la forma en que se obtienen los datos personales que obran en el Sistema o bien si estos provienen de otro Sistema) | | |
|---|---|---|
| ☒ Grafico<br>☐ Electrónico<br>☐ Telefónico<br>☐ Audiovisual<br>☐ Óptico<br>☐ Sonoro<br>☐ En caso de existir otro medio no enlistado, favor de indicar cual<br>_____ | **Indirecta** (obtenida, creada, generada en algún otro sistema) | ☒ |
| | **Señalar cual:**<br>Áreas generadoras del gasto | |

| **7. Responsable del Sistema** Se entiende a la persona Titular de la Unidad Administrativa propietaria del Sistema | |
|---|---|
| Nombre | L.C. Juan Manuel Gallegos Motte |
| Cargo | Subdirector de Finanzas |
| Área de adscripción | Subdirección de Finanzas |
| Teléfono | 55 1084 0900 Exts. 1574, 1279 |
| Correo electrónico | @pediatria.gob.mx |
| Función | Descripción de las atribuciones con relación al tratamiento de los datos personales sistema |
| Obligación | Descripción de las responsabilidades en cuanto al tratamiento de los datos personales del sistema |

| **8. Encargado.** La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras **tratara** datos personales a nombre y cuenta del responsable. | |
|---|---|
| Nombre | |
| Cargo | |
| Área de adscripción | |
| Teléfono | |
| Correo electrónico | |
| Función | |
| Obligación | |

| **9. Propietario del Sistema** La persona que **genera** la información y decide sobre cómo se realiza el tratamiento de los datos personales que tiene asignados, conforme a facultades y atribuciones previstas en el Estatuto Orgánico del Instituto. | |
|---|---|
| Nombre | |
| Cargo | |
| Área de adscripción | |
| Teléfono | |
| Correo electrónico | |
| Función | |
| Obligación | |

| **8. Administrador del Sistema** Se entiende a la parte con facultades para la toma de decisiones que tiene a cargo responsabilidad técnica respecto al sistema quien tiene a su cargo la responsabilidad de la administración del sistema | |
|---|---|
| Nombre | |
| Cargo | |
| Área de adscripción | |
| Teléfono | |
| Correo electrónico | |
| Función | |
| Obligación | |

| **11. Custodio** La persona que se **encarga** de la gestión de activos informáticos, su administración diaria y el monitoreo de la seguridad en los sistemas de tratamiento de datos personales que se encuentran bajo su resguardo. |
|---|

| | |
|---|---|
| Nombre | Misael Tovar Cruz |
| Cargo | Subdirector de Tecnologías de la Información |
| Área de adscripción | Dirección de Planeación |
| Teléfono | 55 1084 0900 Ext 1495 |
| Correo electrónico | mtovarc@pediatria.gob.mx |
| Función | Protección de datos, implementar medidas de seguridad, gestionar incidentes, promover la conciencia de seguridad. Mantener la protección adecuada de la información confidencial.<br><br>Mantener la disponibilidad, confidencialidad e integridad en los datos personales e institucionales |
| Obligación | Articulo 3.- Numero VIII. Atender las disposiciones normativas en materia de protección de datos personales, transparencia y rendición de cuentas;<br><br>e) Considerar medidas de rescisión y/o responsabilidades legales en caso de que los proveedores o su personal transgredan las políticas y acuerdos de confidencialidad o realicen actividades que, sin<br>autorización de la Institución, expongan la información institucional o incumplan con la legislación en<br>materia de protección de datos personales.<br><br>Artículo 67.- Los proyectos de servicios de desarrollo o mantenimiento de software deberán incluir el diseño detallado o conceptual del aplicativo a desarrollar, que comprenda por lo menos:<br><br>c) Políticas de privacidad y protección de datos personales, de conformidad con la legislación aplicable;<br><br>Artículo 69.- Los aplicativos de cómputo que operen sobre datos críticos, confidenciales o sensibles, deberán garantizar que el procesamiento y transferencia de la información se realice a través de mecanismos que garanticen su seguridad e integridad, como priorizar su alojamiento en territorio nacional. Para ello, deberán atender los Estándares Técnicos emitidos por la CEDN, la legislación en materia de protección de datos personales y las disposiciones que sean emitidas en materia de Seguridad Nacional. |

**12. Usuario Genérico** La persona que **utiliza** el sistema de tratamiento de datos personales para interactuar con la información y realizar sus actividades, atendiendo a las medidas de seguridad, así como a la Confidencialidad, Integridad y Disponibilidad de la Información

**Se anexa relación del Personal de la Subdirección de Finanzas.**

| | |
|---|---|
| Nombre | |
| Cargo | |
| Área de adscripción | |
| Teléfono | |
| Correo electrónico | |
| Función | **Estatuto Orgánico** |
| Obligación | **Gestión financiera y Presupuestal** |
| Nivel 2 Subdirección | |

**13. Tipo de soporte de la base de datos y donde se ubica el mismo** (Deberá indicar las características del lugar donde se resguardan los soportes, se deberá otorgar información conforme lo siguiente:

a) **Para soportes físicos**, el sujeto obligado deberá incluir una descripción escrita con detalles sobre las características físicas de la oficina, almacén o bodega donde resguarda dichos soportes;

b) **Para soportes electrónicos**, la descripción ofrecida por el sujeto obligado deberá incluir un diagrama de la arquitectura de seguridad en el cual sea posible apreciar el flujo de datos a través de la o las redes electrónicas que interconectan los equipos (clientes, servidores, cortafuegos, unidades de almacenamiento, entre otros) del sistema. Además, deberá describir las medidas de seguridad física que ha implementado para la protección del centro de datos donde residen tales soportes, y

c) **En caso de que el sistema ocupe ambos tipos de soportes**, deberá presentar las descripciones correspondientes a cada uno, en términos de lo señalado en los incisos a) y b) anteriores)

☐ j) Físico _____

☐ k) Electrónico _____

☒ l) Ambos Archivo físico (papel) y Electrónico (bases de datos)

Base de Datos de los Sistemas y aplicativos, acceso restringido a la red institucional, cortafuegos, centro de datos principal con acceso controlado y restringido con biométrico dactilar, manejo de usuarios con contraseña bajo perfiles de usuario, antivirus, acceso al equipo de cómputo mediante Directorio Activo, discos duros de respaldos asignados al usuario, entre otros.

**14. Realiza transferencias de datos personales** (Entiéndase como la comunicación de datos o entrega total o parcial de los mismos, a cualquier persona distinta a su titular, sea mediante el uso de medios físicos o electrónicos, tales como la interconexión de computadoras o bases de datos, acceso a redes de telecomunicación, así como a través de la utilización de cualquier otra tecnología que lo permita. En el ámbito de la Administración Pública Federal se tienen)

☒ SI ☐ NO

*Describir en que consiste la transferencia conforme a lo siguiente:

☒ 10. Interinstitucionales (Transmisiones de datos a dependencias y entidades de la APF. Entidades federativas y municipios)
☐ 11. Internacionales (Transmisiones gobiernos u organismos internacionales)
☐ 12. Con entes privados u organizaciones civiles públicas o privadas

| ¿Qué datos personales o categorías son transferidos? | ¿A quién son transferidos? | ¿Para qué finalidad son transferidos? |
|---|---|---|
| I, VI | SAT Y TESOFE | PAGO Y CUMPLIMIENTO FISCAL |

**Se requiere consentimiento**

SI ☐ NO ☒

| Supuestos artículos 22, 66 ó 70 que se actualizan en su caso | Tipo de consentimiento que se requiere para la transferencia | La transferencia requiere la suscripción de clausulas contractuales, convenios de colaboración u otro instrumento jurídico. |
|---|---|---|
| 22 FRACCION 1 Y 5 | ☒ Tácito<br>☐ Expreso por escrito | ☐ SI ☒ NO |

**15. Portabilidad de datos** (Indicar si las características del sistema permiten apreciar un sistema de datos personales estructurado comúnmente utilizado.)

| | |
|---|---|
| SI ☐ | NO ☒ |

**16. Difusión de datos personales** (Indicar si en el tratamiento se realiza la difusión de datos personales y su fundamentación)

SI ☐
Fundamento_____

NO ☒

**17. Nivel de protección que requieren los datos** (indicar el nivel aplicable, el cual estará determinado en base a los datos en posesión, siguiendo los criterios internacionales de seguridad para el resguardo eficaz de los mismos. Los

| |
|---|
| niveles de seguridad responden a la mayor o menor necesidad de garantizar la integridad de los datos personales, conforme a lo siguiente) |
| ☒ E. **Nivel Básico. – I** Datos de identificación y autentificación, **II** Datos laborales, **III** Datos de contacto, **V.** Datos relacionados con intereses personales y profesionales |
| ☒ F. **Nivel Medio. - IV.** Datos académicos, **VI.** Datos patrimoniales o financieros, **XII.** Datos de tránsito o migratorios, **XIII.** Aparatos de asistencia o apoyos funcionales, **XIV.** Datos sobre procedimientos administrativos seguido en forma de juicio |
| ☐ C. **Nivel Alto. - VII.** Datos biométricos, **VIII.** Datos genéticos, **IX.** Datos genómicos, **X.** Datos de salud, **XI.** Datos ideológicos |
| **18. Actualización de la información contenida en el sistema (**indicar la frecuencia con que se actualiza la información directamente en la base de datos del sistema) |
| ☒ Diaria ☐ Bimestral ☐ Trimestral ☐ Semestral ☐ Anual ☐ Otra especificar _____ |
| **19. Número de titulares involucrados 56** |
| **20. Plazo de conservación de los datos personales** (indicar cuanto tiempo permanecerán los datos personales en el Sistema de Datos conforme a su vigencia y finalidad, es decir atendiendo al ciclo de vida del trámite o servicio por motivo del cual se obtuvieron, basado en los instrumentos de control archivístico, CADIDO y Cuadro General de Clasificación Archivística) |
| ☒ 6 años ☐ _____ meses ☐ _____ días Otro ☐ especificar_____ |

| Indicar Sección de archivos | Serie de archivo | Subserie de archivo en su caso |
|---|---|---|
| | | |

| | |
|---|---|
| **20. Medidas de Seguridad (**indicar los elementos de seguridad con que se cuenta y se abordan en tres modalidades tomando como base el estándar internacional ISO/IEC 27002:2005 que se refiere a mejores prácticas sobre seguridad de la información) | |
| Físicas | ☒ Portación de credencial institucional<br>☒ Acceso solo a áreas autorizadas<br>☐ Acceso a instalaciones con código numérico o de barras<br>☒ Acceso a instalaciones en base a dato biométrico<br>☒ Puertas con cerradura, cerrojos, chapas. etc<br>☒ Control e identificación de equipos portátiles de usuarios<br>☐ Control e identificación de equipos portátiles de empleados trabajadores<br>☒ Control de llaves<br>☐ Control de apertura y cierre de puertas externas e internas<br>Otro especificar_____ |
| Administrativas | ☒ **Política de seguridad.** Política de Seguridad de la Información<br><br>☒ **Cumplimiento de la normatividad.**<br>**Constitución Política de los Estados Unidos Mexicanos; Plan Nacional de Desarrollo 2019-2024; Ley Orgánica de la Administración Pública Federal; Ley General de Salud; Reglamento Interior de la Secretaría de Salud; Ley de los Institutos Nacionales de Salud; Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, y su Reglamento; Ley de Obras Públicas y Servicios Relacionados con las Mismas, y su Reglamento; Ley Federal de Entidades Paraestatales, y su Reglamento; Presupuesto de Egresos de la Federación (PEF)para el ejercicio fiscal 2023; Ley de Ingresos de la Federación para el ejercicio 2023; General de Contabilidad Gubernamental; Ley Federal de Presupuesto y Responsabilidad Hacendaria, y su Reglamento; Ley Federal de Responsabilidades de los Servidores Públicos; Ley de Tesorería de la Federación y su reglamento; Ley General de Bienes Nacionales; Ley Federal de Austeridad Republicana; Oficios Circulares emitidos por la Subsecretaria de Egresos de la SHCP; Disposiciones Administrativas emitidas por la secretaria de la Función Pública; Clasificador por Objeto Económica, Administrativa y Funcional del Gasto emitido para la Administración Pública Federal por la SHCP; Decreto que establece las Medidas para el Uso Eficiente, Transparente y Eficaz de los Recursos Públicos y las Acciones de la Disciplina Presupuestaría en el ejercicio de Gasto Público, así como para la modernización de la Administración Pública Federal; Lineamientos de Racionalidad y Austeridad Presupuestaria 2023; Estatuto Orgánico del INP; Código de Ética del INP, Contrato de servicios y acuerdo de confidencialidad.** |

| | |
|---|---|
| | **Organización de la seguridad de la información.** Política de Seguridad de la información (Garantizar la confidencialidad, integridad y disponibilidad de la información del INP, a partir del establecimiento de lineamientos, políticas, controles, procedimientos y el fomento de una cultura de seguridad de la información.)<br><br>**Seguridad relacionada a los recursos humanos.** Política De Recursos Humanos (Establecer los lineamientos, en materia de seguridad de la información, sobre el proceso de Recursos Humanos que deben pasar previo a la relación laboral, durante la relación laboral con el Instituto Nacional de Pediatría y una vez que se dé por terminada la relación laboral.)<br><br>**Administración de incidentes.** Plan De Contingencia (Se establece el procedimiento de responsabilidades para la detección, escalado y mitigación de incidentes de seguridad de la información del sistema través de la Subdirección de TI).<br><br>**Continuidad de las operaciones.** Política de Gestión (Establecer los lineamientos, en materia de seguridad de la información, para identificar, detectar, registrar, reportar y atender de forma adecuada y eficaz los incidentes de seguridad de la información con la finalidad de reducir el posible impacto de estos en las operaciones del INP.) Teniendo en cuenta el equipo de protección civil ante desastres naturales |
| Técnicas | **Gestión de comunicaciones y operaciones**. Política de tecnologías Móviles (Establece lineamientos, en materia de seguridad de la información, para prevenir pérdidas, daños, hurtos o el compromiso de los recursos tecnológicos, así como para la seguridad y protección de los equipos de escritorio y portátiles contra amenazas físicas y lógicas.), uso de perfiles de usuario y software antivirus<br><br>**Control de acceso**.<br>Política de administración de la seguridad de la red (Establece los lineamientos, en materia de seguridad de la información, sobre la administración de seguridad de la red y el acceso y restricción a las redes del INP, que permitan asegurar la confidencialidad, integridad y disponibilidad de la información que se transmite a través de estas), Directorio Activo, Perfiles de usuarios en sistemas informáticos<br><br>**Adquisición, desarrollo, uso y mantenimiento de sistemas de información**: Política de Sistemas, Aplicaciones y Servicios (Establece los lineamientos, en materia de seguridad de la información, para mantener la seguridad de la información durante la adquisición, desarrollo y mantenimiento de sistemas, así como establecer lineamientos a seguir por parte de los colaboradores del Instituto Nacional de Pediatría, para asegurar la integración de la seguridad de la información en los sistemas de información actuales y futuros que sean parte del INP.) |

**21. Acceso a instalaciones (**Indicar los elementos que se advierten en el sujeto obligado conforme a lo siguiente)

1. **Seguridad perimetral exterior** (las instalaciones del sujeto obligado)
¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones?
Controles biométricos y portación de credencial

- **Personal que labora en el Instituto Nacional de Pediatría (INP)**
  **Control de acceso biométrico de reconocimiento facial para el personal, portación de credencial Institucional, circuito cerrado de Televisión y personal de vigilancia que se idéntica visualmente con su uniforme**
- **Personal Externo al INP**
  **Se cuenta con registro en ventanilla con el personal de vigilancia, se capturan sus datos y fotografía de la persona a ingresar y se comparte un código de tipo quick response que lo deben de portar durante su visita**
- **Registro de familiares del paciente**
  **Se hace mediante el carnet del paciente**

¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones?
a) ¿Cómo las identifica? **El personal porta la credencial dentro de la institución,**
b) ¿Cómo las autentifica? **Con la inspección visual y monitoreo en el circuito cerrado**
c) ¿Cómo les autoriza el acceso? **Por medio del personal de seguridad cuando se porta la credencial**

2. **Seguridad perimetral interior** (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):
¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? **Se ingresa a partir de una puerta con control biométrico de huella dactilar al centro de datos principal y registro de bitácora, puertas con acceso restringido a los cuartos de comunicación secundarios**

Para las personas que acceden a dichos espacios interiores:
a) ¿Cómo las identifica? **El personal tiene la obligación de portar la credencial en todo momento, huella dactilar en el centro de datos y monitoreo mediante circuito cerrado**
b) ¿Cómo las autentifica? Existen perfiles de acceso al centro de datos por el reconocimiento dactilar, **Se cuenta con circuito cerrado en el hospital**
c) ¿Cómo les autoriza el acceso? **Se asigna al personal del Instituto, registra su entrada con biométrico en el centro de datos, existe una bitácora de acceso y se registra hora, nombre del personal que ingresa, hora de entrada, hora de salida y motivo del ingreso.**

**22. Perfiles de usuario y contraseña**

1. Modelo de control de acceso:
a) ¿Es obligatorio? **Si**
b) ¿Es discrecional? **Si**
c) ¿Está basado en roles (perfiles) o grupos? **Si**
d) ¿Está basado en reglas? **Sí**

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
a) ¿Cuenta con un sistema operativo de red instalado en sus equipos? **Sí**
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas? **Sí**
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? **Solo las contraseñas**

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de datos personales:
a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas? **Sí**
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? **Solo las contraseñas**

4. Administración de perfiles de usuario y contraseñas:
a) ¿Quién da de alta nuevos perfiles? **Administradores (Encargados) del sistema**
b) ¿Quién autoriza la creación de nuevos perfiles? **Jefe Inmediato del Área**
c) ¿Se lleva registro de la creación de nuevos perfiles? **Sí, mediante solicitud escrita**

5. Acceso remoto al sistema de datos personales:
a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? **No**
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? **No**
c) ¿Cómo se evita el acceso remoto no autorizado? **Por restricción de acceso mediante direcciones IP**

**23. Bitácoras de acceso y operación cotidiana, seguridad aplicable**

| | |
|---|---|
| Soporte físico | El administrador del sistema procura el control y registro conforme a lo siguiente:<br>9. Emite la facultad de accesos a los servidores públicos a fin de que este, en el ejercicio de sus funciones puedan interactuar con una o más vistas del sistema, mediante solicitud escrita.<br>10. La asignación, actualización y remplazo de contraseña que se entrega al personal, se realiza en respuesta a la solciitud escrita mediante sobre cerrado al usuario.<br>11.<br>12. Las acciones de los autorizados llevan a cabo en el área de resguardo. Para ello, cada una de las personas realiza un vale para realizar cambios dependiendo la acción.<br>13. El administrador del sistema lleva un control de los cambios realizados.<br>14. Se registra en bitácora de eventos ocurridos mediante vale o solicitud de servicios de sistema, fecha de solicitud, área solicitante, clave y nombre del solicitante, nombre de quien autoriza (jefe inmediato), sistema que se reporta, descripción de la solicitud, fecha de terminación del trámite, firma de conformidad del usuario, firma de quien realizo, firma del jefe del departamento. |
| Soporte electrónico | 1. El Responsable del sistema o área en coordinación con la Subdirección de Tecnologías de la Información lleva un control y registro, conforme a lo siguiente: |

| | |
|---|---|
| | a) Se generan bitácoras de eventos ocurridos a nivel sistema operativo en los equipos (servidores, cortafuegos, almacenamiento masivo) que habilitan la operación del sistema de datos. Entre otras, se generan bitácoras para desempeño del servidor: intentos de acceso (exitosos y fallidos); accesos denegados a usuarios y terminales; uso de herramientas para administración del servidor, y fecha y hora de los eventos anteriores.<br><br>b) Se realiza una bitácora de eventos generados a nivel software aplicativo del sistema de datos personales. Estas bitácoras tienen como registro las actividades de relacionadas con el sistema, si se genera un mensaje de error, acciones de apertura, modificación y cierre de archivos, así como la detención de amenazas de seguridad por parte del software. Cada uno de los eventos configurados en el software quedan registrados.<br><br>c) Control de acceso al equipo de cómputo mediante Directorio Activo |

24. Lugar de almacenamiento de las bitácoras y tiempo de conservación y conservación de integridad (

a) Se garantiza copiándolas en un servidor del centro de datos el cual las graba en CD-R.
Se realiza copia de servidor del centro de datos perteneciente al Instituto Nacional de Pediatría
b) Algunas se copian cada hora, otras a diario
Se realiza copia todos los días y se mantiene un respaldo de cada mes y año
c) La integridad de las copias se garantiza además con "resúmenes" creados por un algoritmo "digestor".
Por el momento no se cuenta con herramienta de software
d) Se cuenta con una herramienta de software que automatiza estas operaciones.
Por el momento no se cuenta con herramienta de software

Especificarse si las áreas de informática y seguridad de la información han designado una persona que se encarga de realizar un análisis de las bitácoras generadas, conforme a lo siguiente:
Si, el Instituto Nacional de Pediatría actualmente cuenta con personal designado para realizar el análisis de bitácoras
a) Se cuenta con la ayuda de una herramienta informática adquirida para tal propósito. No, se encuentra en proceso
b) Cada semana se llevan a cabo análisis de bitácoras, pero no de todas ellas. Depende de la bitácora y de las amenazas detectadas en el entorno. La bitácora y de las amenazas son detectadas en el entorno.

25. Registro de incidentes

Registro de Incidentes en el Sistema Integral De Administración INP (SIA).
1.- Los datos registrados sobre el incidente serán los siguientes:

p) Hora y fecha de incidencia
q) Persona que reporta el incidente
r) Documentación ante incidente (Elaboración de "plan de respuesta a incidente "medidas de seguridad previamente implementadas, identificación de activos, medidas de seguridad de los activos, alertas de seguridad de asociadas a las medidas, propósito de medidas de seguridad para, mitigar el incidente)
s) Registrar si es el incidente es físico o electrónico
t) Documentar como se asegura la integridad de la información mediante el plan de respuesta a incidentes
u) Autorización de recuperación de información por parte del área que reporta
v) Solución del incidente
w) Fecha de conclusión del incidente

Procedimiento en caso de presentarse un incidente.

17. El responsable de seguridad tiene la labor de detectar el incidente
18. El responsable registra y clasifica el incidente del Sistema Integral de Administración (INP).
19. Notifica el incidente al equipo y realiza la revisión de la contención buscando la detección del incidente con el fin de que no se propague y pueda generar más daños a la información o a la arquitectura del SIA
20. El responsable de seguridad genera un informe detallado del incidente a más tardar al día siguiente de lo ocurrido, dicho informe detallará lo ocurrido en el Sistema Integral de Administración (INP).

21. Se documentará el proceso de solución del incidente
22. En caso de pérdida de información de datos personales, el Subdirector de Tecnologías de la Información, al tener conocimiento del incidente de aviso al Director de área para su conocimiento y al titular del área jurídica para presentar denuncia.
23. Después de ocurrir el Incidente se inicia la recuperación, reintegración de activos, monitoreo de nuevas medidas y generación de pruebas de incidente.
24. Posterior a lo ya mencionado se empieza a trabajar sobre la mejora continua, donde se generará documentación final de incidente.

**26. Procedimiento de respaldo y recuperación de datos** (Indicar si es el caso donde los medios de respaldo con que se cuenta, siendo deseable al menos dos lugares distintos que cumplan con las condiciones de seguridad; o bien si se utiliza un espacio externo seguro para guardar de manera sistemática datos y respaldos, conforme a lo siguiente:)

1. Señalar si realiza respaldos completos, diferenciales o incrementales; **Completo**
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad; **Discos duros, Servidor**
3. Cómo y dónde archiva esos medios, **Centro de datos y área de Sistemas de la Información**
4. Quién es el responsable de realizar estas operaciones (el sujeto obligado o un tercero) **El sujeto obligado**

**27. Plan de contingencia** Indicar si se cuenta con un plan de contingencia y si este atiende conforme a lo siguiente:)

3. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.

**Este plan de contingencia se encuentra en desarrollo y documentación para los módulos o subsistemas del Sistema de gestión para las operaciones financieras y presupuestales**

4. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia del mismo.

**En mención de que se encuentra en desarrollo, una vez establecido se llevarán a cabo las pruebas de eficiencia del mismo.**

5. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:
   **El sistema no cuenta con sitio redundante**
   e) El tipo de sitio (caliente, tibio o frío);
      **Es posible habilitar lo módulos o subsistemas en un sitio frio**
   f) Si el sitio es propio o subcontratado con un tercero;
      **Se considera un sitio propio**
   g) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio, y
      **Se considera equipo y recurso humano institucional**
   h) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.
      **Es posible habilitarlo en 120 horas.**

**28. Encargado de datos (**Indicar el Prestador de servicios persona física o moral, pública o privada ajena al INP que sola o conjuntamente con otros, trata datos personales a nombre y por cuenta en subcontratación, conforme a lo siguiente:)

| | | | | |
|---|---|---|---|---|
| Existe un prestador de servicios, persona física o moral, pública o privada ajena al INP que sola o conjuntamente, trate datos personales a nombre y por cuenta de este Instituto | SI | | NO | X |

**29. Plazo de conservación y bloqueo de los datos personales (**periodo en el que la autoridad conservará los datos para efectos de responsabilidades, el cual será equivalente al plazo de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento en términos de la normatividad de aplicable y, cumplido este plazo, deberá procederse a la supresión del dato que implica el borrado físico del mismo, conforme a las siguientes consideraciones:)

a) Deberá considerar lo dispuesto en el Catálogo de disposición documental -un registro general, además, que se debe incluir la siguiente información del Catálogo de disposición documental -un registro general y sistemático que establece los siguientes valores documentales-: (i) los plazos de conservación; (ii) la vigencia documental; (iii) la clasificación de reserva o confidencialidad, y (iv) el destino final de los documentos.

b) Deberá verificar si el mismo tiene valores históricos, científicos, estadísticos o contables. En caso de que contenga dichos valores, los datos personales serán objeto de transferencias secundarias, de conformidad con lo establecido por los catálogos de disposición documenta.

c) Deben atender al valor documental de la información contenida en el mismo, de conformidad con los criterios establecidos por el sujeto obligado en consideración a la posible consulta que de los mismos se requiriera o a cualquier otra implicación jurídica que pudiera existir en razón de la normatividad aplicable.

| | |
|---|---|
| 0. Unidad De Gestión Médico Financiera | Fecha de Elaboración (mes y año): Junio 2024<br>Fecha última Actualización (mes y año): Junio 2024 |
| 1. Nombre del Sistema | Sistema de Gestión Financiera (SIGMEFI) |
| 2. Objetivo | 1) Resguardar la información respecto a la seguridad social de los pacientes, indicando si tienen derecho o no a atención médica gratuita.<br>2) Imprimir formato de gratuidad, para uso en Cajas o Cuentas Corrientes |
| 3. Fundamento Legal | 1) ARTÍCULO 77 BIS 7 DE LA LEY GENERAL DE SALUD<br><br>Para que las personas puedan acceder a la prestación gratuita de los servicios de salud, medicamentos y demás insumos asociados a que se refiere el presente Título, se deberán reunir los siguientes requisitos:<br><br>I. Encontrarse en territorio nacional;<br><br>II. No ser derechohabiente de las instituciones de seguridad social;<br><br>III. Contar con Clave Única de Registro de Población.<br><br>En caso de no contar con dicha clave, podrá presentarse acta de nacimiento, certificado de nacimiento o los documentos que se establezcan en las disposiciones reglamentarias, y<br><br>IV. Servicios de Salud del Instituto Mexicano del Seguro Social para el Bienestar (IMSS-BIENESTAR) podrá establecer, a través de campañas, universos de personas beneficiarias en atención a las necesidades de cada grupo.<br><br>2) DOF. ACUERDO por el que se modifica el diverso por el que se emiten los criterios generales y la metodología a los que deberán sujetarse los procesos de clasificación socioeconómica de pacientes en los establecimientos que presten servicios de atención médica de la Secretaría de Salud y de las entidades coordinadas por dicha Secretaría, publicado el 27 de mayo de 2013.<br><br>3) POLÍTICAS RELACIONADAS A GRATUIDAD, SEGURIDAD SOCIAL Y CASOS ESPECIALES |

4. DATOS PERSONALES QUE CONTIENE EL SISTEMA

✖ I. Datos de identificación y autentificación

✖ III. Datos de contacto y ubicación

5. FINALIDADES PARA LOS QUE SON TRATADOS LOS DATOS PERSONALES RECABADOS Y SI REQUIERE CONSENTIMIENTO

✖ Para determinar si el paciente tiene derecho o no a la atención médica gratuita, en base a lo dispuesto en la Ley General de Salud.

| Requiere consentimiento | Supuesto artículo 22, que se actualiza en su caso | Tipo de consentimiento |
|---|---|---|
| ✖ No | Artículo 22. El responsable no estará obligado a recabar el consentimiento del titular para el tratamiento de sus datos personales en los siguientes casos: | ✖ Tácito<br>☐ Expreso<br>☐ Expreso por escrito |

| | | |
|---|---|---|
| | ✖ I. Cuando una ley así lo disponga, debiendo dichos supuestos ser acordes con las bases, principios y disposiciones establecidos en esta Ley, en ningún caso, podrán contravenirla;<br>☐ II. Cuando las transferencias que se realicen entre responsables, sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;<br>☐ III. Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;<br>☐ IV. Para el reconocimiento o defensa de derechos del titular ante autoridad competente;<br>☐ V. Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;<br>☐ VI. Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;<br>☐ VII. Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico, la prestación de asistencia sanitaria;<br>☐ VIII. Cuando los datos personales figuren en fuentes de acceso público<br>☐ IX. Cuando los datos personales se sometan a un procedimiento previo de disociación, o<br>☐ X. Cuando el titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley en la materia | |

**6.FORMA DE OBTENCIÓN DE LOS DATOS PERSONALES** (Indicar la forma en que se obtienen los datos personales que obran en el Sistema o bien si estos provienen de otro Sistema)

| | | |
|---|---|---|
| ✖ Grafico<br>✖ Electrónico<br>Telefónico<br>Audiovisual<br>Óptico<br>Sonoro<br>En caso de existir otro medio no enlistado, favor de indicar cual<br>_____ | **Indirecta** (obtenida, creada, generada en algún otro sistema) | ✖ Obtenida |
| | **Señalar cual:** Derechohabiencia al IMSS e ISSSTE de los pacientes, por medio de la Plataforma "AAMATES Derechohabiencia" | |

**7. Responsable del Sistema** Se entiende a la persona Titular de la Unidad Administrativa propietaria del Sistema

| | |
|---|---|
| Nombre | Dr. Ernesto Rubén Cerón Ramírez |
| Cargo | Encargado de la Unidad de Gestión Médico Financiera |
| Área de adscripción | Dirección de Administración |
| Teléfono | 55 1084 0900 Ext. 2011 |
| Correo electrónico | eceronr@pediatria.gob.mx |
| Función | Resguardo de la información comprobatoria del trámite de gratuidad |

| | |
|---|---|
| Obligación | Resguardo de la información comprobatoria del trámite de gratuidad |
| **8. Encargado.** La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras **tratara** datos personales a nombre y cuenta del responsable. | |
| Nombre | |
| Cargo | |
| Área de adscripción | |
| Teléfono | |
| Correo electrónico | |
| Función | |
| Obligación | |
| **9. Propietario del Sistema** La persona que **genera** la información y decide sobre cómo se realiza el tratamiento de los datos personales que tiene asignados, conforme a facultades y atribuciones previstas en el Estatuto Orgánico del Instituto. | |
| Nombre | |
| Cargo | |
| Área de adscripción | |
| Teléfono | |
| Correo electrónico | |
| Función | |
| Obligación | |
| **10. Administrador** La persona responsable de **otorgar** permisos y vigilar la ejecución de actividades asignadas a los usuarios genéricos. | |
| Nombre | |
| Cargo | |
| Área de adscripción | |
| Teléfono | |
| Correo electrónico | |
| Función | |
| Obligación | |
| **11. Custodio** La persona que se **encarga** de la gestión de activos informáticos, su administración diaria y el monitoreo de la seguridad en los sistemas de tratamiento de datos personales que se encuentran bajo su resguardo. | |
| Nombre | Ing. Misael Teofilo Tovar Cruz |
| Cargo | Subdirector de Tecnologías de la Información |
| Área de adscripción | Dirección de Planeación |
| Teléfono | 55 1084 0900 Ext 1495 |
| Correo electrónico | mtovarc@pediatria.gob.mx |
| Función | Protección de datos, implementar medidas de seguridad, gestionar incidentes, promover la conciencia de seguridad. Mantener la protección adecuada de la información confidencial.<br><br>Mantener la disponibilidad, confidencialidad e integridad en los datos personales e institucionales. |
| Obligación | Articulo 3.- Numero VIII. Atender las disposiciones normativas en materia de protección de datos personales, transparencia y rendición de cuentas;<br><br>e) Considerar medidas de rescisión y/o responsabilidades legales en caso de que los proveedores o su personal transgredan las políticas y acuerdos de confidencialidad o realicen actividades que, sin<br>autorización de la Institución, expongan la información institucional o incumplan con la legislación en<br>materia de protección de datos personales.<br><br>Artículo 67.- Los proyectos de servicios de desarrollo o mantenimiento de software deberán incluir el diseño detallado o conceptual del aplicativo a desarrollar, que comprenda por lo menos:<br><br>c) Políticas de privacidad y protección de datos personales, de conformidad con la legislación aplicable; |

| | |
|---|---|
| | Artículo 69.- Los aplicativos de cómputo que operen sobre datos críticos, confidenciales o sensibles, deberán garantizar que el procesamiento y transferencia de la información se realice a través de mecanismos que garanticen su seguridad e integridad, como priorizar su alojamiento en territorio nacional. Para ello, deberán atender los Estándares Técnicos emitidos por la CEDN, la legislación en materia de protección de datos personales y las disposiciones que sean emitidas en materia de Seguridad Nacional. |
| **12. Usuario Genérico** La persona que **utiliza** el sistema de tratamiento de datos personales para interactuar con la información y realizar sus actividades, atendiendo a las medidas de seguridad, así como a la Confidencialidad, Integridad y Disponibilidad de la Información | |
| **Usuarios del Sistema SIGMEFI:** | |
| Nombre | 1) Aura Nallely Rodríguez Vázquez<br>2) Bárbara Vergara Rojano<br>3) Beatriz Moreno Gómez<br>4) Diego Chavelas Magaña<br>5) Elías Luna de Paz<br>6) Julio Alexander Zavala Soria<br>7) Juana Alejandra López Carmona<br>8) Karen Andrea de la Cruz Moreno<br>9) María Laura Trejo Gómez<br>10) Norma Angélica Mendoza González<br>11) Óscar Ernesto Cruz Rosas<br>12) Priscila Denisse Landeros Castillo<br>13) Raúl Alberto Collado Padilla |
| Cargo | 1) Soporte administrativo<br>2) Apoyo Administrativo<br>3) Apoyo Administrativo<br>4) Soporte Administrativo<br>5) Soporte Administrativo<br>6) Soporte Administrativo<br>7) Soporte Administrativo<br>8) Soporte Administrativo<br>9) Apoyo Administrativo<br>10) Soporte Administrativo<br>11) Soporte Administrativo<br>12) Soporte Administrativo<br>13) Soporte Administrativo |
| Área de adscripción | Unidad de Gestión Médico Financiera |
| Teléfono | 5510840900 Ext. 1731,1415 o 1890 |
| Correo electrónico | 1) anrodriguezv@pediatria.gob.mx<br>2) bvergarar@pediatria.gob.mx<br>3) bmoreno@pediatria.gob.mx<br>4) dchavelasm@pediatria.gob.mx<br>5) elunad@pediatria.gob.mx<br>6) jzavalas@pediatria.gob.mx<br>7) jlopezc@pediatria.gob.mx<br>8) kdelacrum@pediatria.gob.mx<br>9) mtrejo@pediatria.gob.mx<br>10) nmendoza@pediatria.gob.mx<br>11) ocruzr@pediatria.gob.mx<br>12) planderosc@pediatria.gob.mx<br>13) rcolladop@pediatria.gob.mx |
| Función | 1) Apoyo administrativo del proceso de Gratuidad<br>2) Gestor administrativo del proceso de Gratuidad<br>3) Gestor administrativo del proceso de Gratuidad<br>4) Coordinador del proceso de Gratuidad<br>5) Gestor administrativo del proceso de Gratuidad<br>6) Gestor administrativo del proceso de Gratuidad<br>7) Gestor administrativo del proceso de Gratuidad<br>8) Apoyo administrativo del proceso de Gratuidad |

| | |
|---|---|
| | 9) Apoyo administrativo del proceso de Gratuidad<br>10) Apoyo administrativo del proceso de Gratuidad<br>11) Apoyo administrativo del proceso de Gratuidad<br>12) Apoyo administrativo del proceso de Gratuidad<br>13) Gestor administrativo del proceso de Gratuidad |
| Obligación | Captura y carga de la información del trámite de gratuidad |
| Nivel 2 Subdirección | |

**13. Tipo de soporte de la base de datos y donde se ubica el mismo** (Deberá indicar las características del lugar donde se resguardan los soportes, se deberá otorgar información conforme lo siguiente:

Soportes físicos y electrónicos

✖ a) Físico: Resguardo de dos años del documento "Control de Gratuidad" firmado, en las oficinas de la Unidad de Gestión Médico Financiera, a un costado de la entrada de la Dirección de Administración, cuya entrada y salida está a cargo por un vigilante externo.

✖ b) Electrónico: Resguardo digital de SIGMEFI en el equipo de cómputo del Coordinador de Gratuidad, que está en la Sala B, y se ingresa con contraseña personal del coordinador, Base de Datos de los Sistemas y aplicativos, acceso restringido a la red institucional, cortafuegos, centro de datos principal con acceso controlado y restringido con biométrico dactilar, manejo de usuarios con contraseña bajo perfiles de usuario, antivirus, acceso al equipo de cómputo mediante Directorio Activo, discos duros de respaldos asignados al usuario, entre otros.

**14. Realiza transferencias de datos personales** (Entiéndase como la comunicación de datos o entrega total o parcial de los mismos, a cualquier persona distinta a su titular, sea mediante el uso de medios físicos o electrónicos, tales como la interconexión de computadoras o bases de datos, acceso a redes de telecomunicación, así como a través de la utilización de cualquier otra tecnología que lo permita. En el ámbito de la Administración Pública Federal se tienen)

☐ SI ✖NO

*Describir en que consiste la transferencia conforme a lo siguiente:

☐ 13. Interinstitucionales (Transmisiones de datos a dependencias y entidades de la APF. Entidades federativas y municipios)
☐ 14. Internacionales (Transmisiones gobiernos u organismos internacionales)
☐ 15. Con entes privados u organizaciones civiles públicas o privadas

| ¿Qué datos personales o categorías son transferidos? | ¿A quién son transferidos? | ¿Para qué finalidad son transferidos? |
|---|---|---|
| | | |

**Se requiere consentimiento**

SI ☐ NO ☐

| Supuestos artículos 22, 66 ó 70 que se actualizan en su caso | Tipo de consentimiento que se requiere para la transferencia | La transferencia requiere la suscripción de cláusulas contractuales, convenios de colaboración u otro instrumento jurídico. |
|---|---|---|
| | ☐ Tácito<br>☐ Expreso por escrito | ☐ SI ☐ NO |

**15. Portabilidad de datos** (Indicar si las características del sistema permiten apreciar un sistema de datos personales estructurado comúnmente utilizado.)

| | |
|---|---|
| SI ☐ | NO ✖ |

**16. Difusión de datos personales** (Indicar si en el tratamiento se realiza la difusión de datos personales y su fundamentación)

SI ☐
Fundamento_____

NO ✖

**17. Nivel de protección que requieren los datos** (indicar el nivel aplicable, el cual estará determinado en base a los datos en posesión, siguiendo los criterios internacionales de seguridad para el resguardo eficaz de los mismos. Los niveles de seguridad responden a la mayor o menor necesidad de garantizar la integridad de los datos personales, conforme a lo siguiente)

✖ G. **Nivel Básico. – I** Datos de identificación y autentificación

☐ H. **Nivel Medio. –** ninguno

☐ C. **Nivel Alto. –** ninguno

**18. Actualización de la información contenida en el sistema (**indicar la frecuencia con que se actualiza la información directamente en la base de datos del sistema)

✖ Diaria ☐ Bimestral ☐ Trimestral ☐ Semestral ☐ Anual ☐ Otra especificar _____

**19. Plazo de conservación de los datos personales** (indicar cuanto tiempo permanecerán los datos personales en el Sistema de Datos conforme a su vigencia y finalidad, es decir atendiendo al ciclo de vida del trámite o servicio por motivo del cual se obtuvieron, basado en los instrumentos de control archivístico, CADIDO y Cuadro General de Clasificación Archivística)

✖ __2__ años ☐_____ meses __☐_____ días Otro especificar_____

| Indicar Sección de archivos CADIDO | Serie de archivo | Subserie de archivo en su caso |
|---|---|---|
| 5 | 5C Recursos Financieros | 5C.2 Programas y proyectos en materia de Recursos Financieros y Contabilidad Gubernamental |

**20. Medidas de Seguridad** (indicar los elementos de seguridad con que se cuenta y se abordan en tres modalidades tomando como base el estándar internacional ISO/IEC 27002:2005 que se refiere a mejores prácticas sobre seguridad de la información)

| | |
|---|---|
| Físicas | ✖Portación de credencial institucional<br>✖Acceso solo a áreas autorizadas<br>☐ Acceso a instalaciones con código numérico o de barras<br>✖Acceso a instalaciones en base a dato biométrico<br>✖Puertas con cerradura, cerrojos, chapas. etc<br>☐ Control e identificación de equipos portátiles de usuarios<br>✖Control e identificación de equipos portátiles de empleados trabajadores<br>✖Control de llaves<br>✖Control de apertura y cierre de puertas externas e internas |
| Administrativas | ☐ **Política de seguridad.**: Código de Conducta, Código de Ética y Política general de Seguridad de la Información<br><br>☐**Cumplimiento de la normatividad. Contrato de servicios y Acuerdo de confidencialidad**<br><br>☐**Organización de la seguridad de la información.** Política de Seguridad de la información (Garantizar la confidencialidad, integridad y disponibilidad de la información del INP, a partir del establecimiento de lineamientos, políticas, controles, procedimientos y el fomento de una cultura de seguridad de la información.) |

| | |
|---|---|
| | ◘ **Seguridad relacionada a los recursos humanos.** Política De Recursos Humanos (Establecer los lineamientos, en materia de seguridad de la información, sobre el proceso de Recursos Humanos que deben pasar previo a la relación laboral, durante la relación laboral con el Instituto Nacional de Pediatría y una vez que se dé por terminada la relación laboral.)<br><br>◘**Administración de incidentes.** Plan De Contingencia (Se establece el procedimiento de responsabilidades para la detección, escalado y mitigación de incidentes de seguridad de la información del sistema través de la Subdirección de TI).<br><br>◘ **Continuidad de las operaciones.** Política de Gestión (Establecer los lineamientos, en materia de seguridad de la información, para identificar, detectar, registrar, reportar y atender de forma adecuada y eficaz los incidentes de seguridad de la información con la finalidad de reducir el posible impacto de estos en las operaciones del INP.) Teniendo en cuenta el equipo de protección civil ante desastres naturales |
| Técnicas | ◘ **Gestión de comunicaciones y operaciones**. Política de tecnologías Móviles (Establece lineamientos, en materia de seguridad de la información, para prevenir pérdidas, daños, hurtos o el compromiso de los recursos tecnológicos, así como para la seguridad y protección de los equipos de escritorio y portátiles contra amenazas físicas y lógicas.), uso de perfiles de usuario y software antivirus<br><br>◘ **Control de acceso**.<br>Política de administración de la seguridad de la red (Establece los lineamientos, en materia de seguridad de la información, sobre la administración de seguridad de la red y el acceso y restricción a las redes del INP, que permitan asegurar la confidencialidad, integridad y disponibilidad de la información que se transmite a través de estas), Directorio Activo, Perfiles de usuarios en sistemas informáticos<br><br>◘ **Adquisición, desarrollo, uso y mantenimiento de sistemas de información**: Política de Sistemas, Aplicaciones y Servicios (Establece los lineamientos, en materia de seguridad de la información, para mantener la seguridad de la información durante la adquisición, desarrollo y mantenimiento de sistemas, así como establecer lineamientos a seguir por parte de los colaboradores del Instituto Nacional de Pediatría, para asegurar la integración de la seguridad de la información en los sistemas de información actuales y futuros que sean parte del INP.) |

**21. Acceso a instalaciones** (Indicar los elementos que se advierten en el sujeto obligado conforme a lo siguiente)

1. **Seguridad perimetral exterior** (las instalaciones del sujeto obligado)
¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones?
Controles biométricos y portación de credencial

- **Personal que labora en el Instituto Nacional de Pediatría (INP)**
  **Control de acceso biométrico de reconocimiento facial para el personal, portación de credencial Institucional, circuito cerrado de Televisión y personal de vigilancia que se idéntica visualmente con su uniforme**
- **Personal Externo al INP**
  **Se cuenta con registro en ventanilla con el personal de vigilancia, se capturan sus datos y fotografía de la persona a ingresar y se comparte un código de tipo quick response que lo deben de portar durante su visita**
- **Registro de familiares del paciente**
  **Se hace mediante el carnet del paciente**

¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones?
a) ¿Cómo las identifica? **El personal porta la credencial dentro de la institución,**
b) ¿Cómo las autentifica? **Con la inspección visual y monitoreo en el circuito cerrado**
c) ¿Cómo les autoriza el acceso? **Por medio del personal de seguridad cuando se porta la credencial**

2. **Seguridad perimetral interior** (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):
¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? **Se ingresa a partir de una puerta con control biométrico de huella dactilar al centro de datos principal y registro de bitácora, puertas con acceso restringido a los cuartos de comunicación secundarios**
Para las personas que acceden a dichos espacios interiores:
a) ¿Cómo las identifica? **El personal tiene la obligación de portar la credencial en todo momento, huella dactilar en el centro de datos y monitoreo mediante circuito cerrado**

b) ¿Cómo las autentifica? Existen perfiles de acceso al centro de datos por el reconocimiento dactilar, **Se cuenta con circuito cerrado en el hospital**
c) ¿Cómo les autoriza el acceso? **Se asigna al personal del Instituto, registra su entrada con biométrico en el centro de datos, existe una bitácora de acceso y se registra hora, nombre del personal que ingresa, hora de entrada, hora de salida y motivo del ingreso.**

**22. Perfiles de usuario y contraseña**

1. Modelo de control de acceso:
a) ¿Es obligatorio? **Si**
b) ¿Es discrecional? **Si**
c) ¿Está basado en roles (perfiles) o grupos? **Si**
d) ¿Está basado en reglas? **Sí**

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
a) ¿Cuenta con un sistema operativo de red instalado en sus equipos? **Sí**
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas? **Sí**
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? **Solo las contraseñas**

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de datos personales:
a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas? **Sí**
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? **Solo las contraseñas**

4. Administración de perfiles de usuario y contraseñas:
a) ¿Quién da de alta nuevos perfiles? **Administradores (Encargados) del sistema**
b) ¿Quién autoriza la creación de nuevos perfiles? **Jefe Inmediato del Área**
c) ¿Se lleva registro de la creación de nuevos perfiles? **Sí, mediante solicitud escrita**

5. Acceso remoto al sistema de datos personales:
a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? **No**
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? **No**
c) ¿Cómo se evita el acceso remoto no autorizado? **Por restricción de acceso mediante direcciones IP**

**23. Bitácoras de acceso y operación cotidiana, seguridad aplicable**

| | |
|---|---|
| Soporte físico | El administrador del sistema procura el control y registro conforme a lo siguiente:<br>15. Emite la facultad de accesos a los servidores públicos a fin de que este, en el ejercicio de sus funciones puedan interactuar con una o más vistas del sistema, mediante solicitud escrita.<br>16. La asignación, actualización y remplazo de contraseña que se entrega al personal, se realiza en respuesta a la solicitud escrita mediante sobre cerrado al usuario.<br>17. Las acciones de los autorizados llevan a cabo en el área de resguardo. Para ello, cada una de las personas realiza un vale para realizar cambios dependiendo la acción.<br>18. El administrador del sistema lleva un control de los cambios realizados.<br>19. Se registra en bitácora de eventos ocurridos mediante vale o solicitud de servicios de sistema, fecha de solicitud, área solicitante, clave y nombre del solicitante, nombre de quien autoriza (jefe inmediato), sistema que se reporta, descripción de la solicitud, fecha de terminación del trámite, firma de conformidad del usuario, firma de quien realizo, firma del jefe del departamento. |
| Soporte electrónico | 1. El Responsable del sistema en coordinación con la Subdirección de Tecnologías de la Información lleva un control y registro, conforme a lo siguiente:<br><br>a) Se generan bitácoras de eventos ocurridos a nivel sistema operativo en los equipos (servidores, cortafuegos, almacenamiento masivo) que habilitan la operación del sistema de datos. Entre otras, se generan bitácoras para desempeño del servidor: intentos de acceso (exitosos y fallidos); |

| | |
|---|---|
| | accesos denegados a usuarios y terminales; uso de herramientas para administración del servidor, y fecha y hora de los eventos anteriores.<br><br>b) Se realiza una bitácora de eventos generados a nivel software aplicativo del sistema de datos personales. Estas bitácoras tienen como registro las actividades de relacionadas con el sistema, si se genera un mensaje de error, acciones de apertura, modificación y cierre de archivos, así como la detención de amenazas de seguridad por parte del software. Cada uno de los eventos configurados en el software quedan registrados. |

**24. Lugar de almacenamiento de las bitácoras y tiempo de conservación y conservación de integridad** (Indicar lugar donde reside la bitácora sea físico o electrónico y como se mantiene la integridad de las bitácoras, conforme a lo siguiente:)

a) Se garantiza copiándolas en un servidor del centro de datos el cual las graba en CD-R.
Se realiza copia de servidor del centro de datos perteneciente al Instituto Nacional de Pediatría
b) Algunas se copian cada hora, otras a diario
Se realiza copia todos los días y se mantiene un respaldo de cada mes y año
c) La integridad de las copias se garantiza además con "resúmenes" creados por un algoritmo "digestor".
Por el momento no se cuenta con herramienta de software
d) Se cuenta con una herramienta de software que automatiza estas operaciones.
Por el momento no se cuenta con herramienta de software

Especificarse si las áreas de informática y seguridad de la información han designado una persona que se encarga de realizar un análisis de las bitácoras generadas, conforme a lo siguiente:
Si, el Instituto Nacional de Pediatría actualmente cuenta con personal designado para realizar el análisis de bitácoras
a) Se cuenta con la ayuda de una herramienta informática adquirida para tal propósito. No, se encuentra en proceso
b) Cada semana se llevan a cabo análisis de bitácoras, pero no de todas ellas. Depende de la bitácora y de las amenazas detectadas en el entorno. La bitácora y de las amenazas son detectadas en el entorno.

**25. Registro de incidentes**

Registro de Incidentes en el Sistema de Gestión Financiera.
1.- Los datos registrados sobre el incidente serán los siguientes:

x) Hora y fecha de incidencia
y) Persona que reporta el incidente
z) Documentación ante incidente (Elaboración de "plan de respuesta a incidente "medidas de seguridad previamente implementadas, identificación de activos, medidas de seguridad de los activos, alertas de seguridad de asociadas a las medidas, propósito de medidas de seguridad para, mitigar el incidente)
aa) Registrar si es el incidente es físico o electrónico
bb) Documentar como se asegura la integridad de la información mediante el plan de respuesta a incidentes
cc) Autorización de recuperación de información por parte del área que reporta
dd) Solución del incidente
ee) Fecha de conclusión del incidente

Procedimiento en caso de presentarse un incidente.

25. El responsable de seguridad tiene la labor de detectar el incidente
26. El responsable registra y clasifica el incidente del Sistema de Gestión Financiera.
27. Notifica el incidente al equipo y realiza la revisión de la contención buscando la detección del incidente con el fin de que no se propague y pueda generar más daños a la información o a la arquitectura del Sistema de Gestión Financiera
28. El responsable de seguridad genera un informe detallado del incidente a más tardar al día siguiente de lo ocurrido, dicho informe detallará lo ocurrido en el Sistema de Gestión Financiera
29. Se documentará el proceso de solución del incidente
30. En caso de pérdida de información de datos personales, el Subdirector de Tecnologías de la Información, al tener conocimiento del incidente de aviso al Director de área para su conocimiento y al titular del área jurídica para presentar denuncia.

31. **Después de ocurrir el Incidente se inicia la recuperación, reintegración de activos, monitoreo de nuevas medidas y generación de pruebas de incidente.**
32. **Posterior a lo ya mencionado se empieza a trabajar sobre la mejora continua, donde se generará documentación final de incidente.**

**26. Procedimiento de respaldo y recuperación de datos**

1. Señalar si realiza respaldos completos, diferenciales o incrementales; **Completo**
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad; **Discos duros, Servidor**
3. Cómo y dónde archiva esos medios, **Centro de datos y área de Sistemas de la Información**
4. Quién es el responsable de realizar estas operaciones (el sujeto obligado o un tercero) **El sujeto obligado**

**27. Plan de contingencia** Indicar si se cuenta con un plan de contingencia y si este atiende conforme a lo siguiente:)

6. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.

**Este plan de contingencia se encuentra en desarrollo para el Sistema de Gestión Financiero**

7. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia del mismo.

**En mención de que se encuentra en desarrollo, una vez establecido se llevarán a cabo las pruebas de eficiencia del mismo.**

8. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:
   **El sistema no cuenta con sitio redundante**
   i) El tipo de sitio (caliente, tibio o frío);
   **Es posible habilitar lo módulos o subsistemas en un sitio frio**
   j) Si el sitio es propio o subcontratado con un tercero;
   **Se considera un sitio propio**
   k) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio, y
   **Se considera equipo y recurso humano institucional**
   l) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.
   **Es posible habilitarlo en 48 horas.**

**28. Encargado de datos (**Indicar el Prestador de servicios persona física o moral, pública o privada ajena al INP que sola o conjuntamente con otros, trata datos personales a nombre y por cuenta en subcontratación, conforme a lo siguiente:)

| | | | | |
|---|---|---|---|---|
| Existe un prestador de servicios, persona física o moral, pública o privada ajena al INP que sola o conjuntamente, trate datos personales a nombre y por cuenta de este Instituto | SI | | NO | X |

**29. Plazo de conservación y bloqueo de los datos personales (**periodo en el que la autoridad conservará los datos para efectos de responsabilidades, el cual será equivalente al plazo de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento en términos de la normatividad de aplicable y, cumplido este plazo, deberá procederse a la supresión del dato que implica el borrado físico del mismo, conforme a las siguientes consideraciones:)

Los documentos que se resguardan bajo la clasificación del Catálogo de disposición Documental
Sección 5C. Recursos Financieros
Sud serie 5C.2 programas y Proyectos en Material de Recursos Financieros y Contabilidad Gubernamental.
Todos los documentos que se manejan se dividen de la siguiente manera:
Archivo de trámite se resguardan 2 años
Después del plazo, continúa procedimiento establecido

**Información:** Unidad de Transparencia.

**Diseño:** Subdirección de Tecnologías de la Información.