SISTEMA DE GESTIÓN

Mayo de 2022

INSTITUTO NACIONAL DE CARDIOLOGÍA

IGNACIO CHÁVEZ

Contenido

[I. GLOSARIO DE TÉRMINOS COMUNES 1](#_Toc107229366)

[II. MARCO JURÍDICO 6](#_Toc107229367)

[III. OBJETIVO 7](#_Toc107229368)

[IV. POLÍTICAS INTERNAS DE PROTECCIÓN DE DATOS PERSONALES 8](#_Toc107229369)

[V. PROGRAMA GENERAL DE DATOS PERSONALES 13](#_Toc107229370)

[VI. MEDIDAS DE SEGURIDAD 15](#_Toc107229371)

[VII. TRANSFERENCIA DE DATOS PERSONALES 16](#_Toc107229372)

[VIII. REMISIÓN DE DATOS PERSONALES 22](#_Toc107229373)

[IX. EJERCICIO DE LOS DERECHOS ARCO 25](#_Toc107229374)

[X. CÓMPUTO EN LA NUBE 26](#_Toc107229375)

[XI. PORTABILIDAD DE DATOS PERSONALES 29](#_Toc107229376)

[XII. CICLO DE VIDA DE LOS DATOS PERSONALES 31](#_Toc107229377)

[XIII. EVALUACIÓN EN LA PROTECCIÓN DE DATOS PERSONALES 33](#_Toc107229378)

[XIV. CAPACITACIÓN DE LOS SERVIDORES PÚBLICOS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES 36](#_Toc107229379)

INTRODUCCIÓN

Los artículos 34 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Ley General) y 65 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales), establecen que las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión.

De acuerdo con dicha Ley, el sistema de gestión es el conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales; asimismo, este deberá permitir planificar, establecer, implementar, operar, monitorear, mantener, revisar y mejorar las medidas de seguridad de carácter administrativo, físico y técnico aplicadas a los datos personales; tomando en consideración los estándares nacionales e internacionales en materia de protección de datos personales y seguridad.

El Instituto Nacional de Cardiología Ignacio Chávez, al ser un organismo público descentralizado de la Administración Pública Federal, que tiene por objeto principal, en el campo de la atención de padecimientos cardiovasculares, la investigación científica, la formación y capacitación de recursos humanos calificados y la prestación de servicios de atención médica de alta especialidad, es responsable del tratamiento de los datos personales que le sean proporcionados para los fines antes descritos.

Por lo anterior, el Instituto debe establecer y mantener las medidas de seguridad necesarias para la protección de datos personales, por lo que se presenta el Sistema de gestión de seguridad de datos personales.

# I. GLOSARIO DE TÉRMINOS COMUNES

Área: Instancias del Instituto Nacional de Cardiología Ignacio Chávez, que dan tratamiento a datos personales a las que se les confieren atribuciones específicas en el Estatuto Orgánico del Instituto Nacional de Cardiología Ignacio Chávez, Manual de Organización Específico y Manuales de Procedimientos Internos.

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias y evaluarlas de manera objetiva para determinar el grado de cumplimiento de los criterios preestablecidos para la misma.

Aviso de privacidad: Documento de forma física, electrónica o en cualquier formato, que es generado por el responsable y puesto a disposición de los titulares de los datos personales, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos.

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.

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

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

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: La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable.

Evaluación de impacto en la protección de datos personales: Evaluación mediante la 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.

INAI: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

INC: Instituto Nacional de Cardiología Ignacio Chávez.

Ley General: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Lineamientos Generales: Lineamientos Generales de Protección de Datos Personales para el Sector Público.

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:

1. Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
2. Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
3. Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y
4. 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:

1. Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;
2. Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
3. Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y
4. Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Portabilidad de datos personales: Prerrogativa del titular de obtener una copia de los datos que ha proporcionado al responsable del tratamiento en un formato estructurado que le permita seguir utilizándolos.

Programa: Programa de Protección de Datos Personales.

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

Responsable: Para efectos del presente programa el Instituto Nacional de Cardiología Ignacio Chávez, de conformidad con el artículo 1 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados que deciden sobre el tratamiento de datos personales.

Revisión: Actividad estructurada, objetiva y documentada, llevada a cabo con la finalidad de constatar el cumplimiento continuo de los contenidos establecidos en este Programa.

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

Sistema de gestión: Conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y medidas de seguridad de carácter administrativo, físico y técnico aplicadas a los datos personales, de conformidad con lo previsto en la presente Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y las demás disposiciones que le resulten aplicables en la materia.

Sistema de 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.

SNT: Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Sujeto obligado: Para efectos del presente programa, el Instituto Nacional de Cardiología Ignacio Chávez.

Titular: La persona física a quien corresponden los datos personales.

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

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

Unidad de Transparencia: Instancia a la que hace referencia el artículo 45 de la Ley General de Transparencia y Acceso a la Información Pública.

# II. MARCO JURÍDICO

* Constitución Política de los Estados Unidos Mexicanos (DOF. 05/02/1917 y sus reformas).
* Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (DOF. 26/01/2017).
* Ley General de Transparencia y Acceso a la Información Pública (DOF. 04/05/2015 y sus reformas).
* Ley Federal de Transparencia y Acceso a la Información Pública (DOF. 09/05/2016 y sus reformas).

# III. OBJETIVO

Los objetivos del Sistema de gestión de seguridad de datos personales son los siguientes:

1. Determinar el conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales al interior del Instituto Nacional de Cardiología Ignacio Chávez.
2. Establecer las acciones relacionadas con las medidas de seguridad de carácter administrativo, físico y técnico aplicadas al tratamiento de los datos personales al interior del Instituto Nacional de Cardiología Ignacio Chávez.

# IV. POLÍTICAS INTERNAS DE PROTECCIÓN DE DATOS PERSONALES

El derecho a la protección de los datos personales es un derecho humano reconocido en los artículos 6 y 16 de la Constitución Política de los Estados Unidos Mexicanos, así como en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, que imponen obligaciones a los RESPONSABLES que tratan datos personales, y que reconoce derechos a los TITULARES de los datos, a fin de garantizar su privacidad, el buen uso de la información personal y el derecho a decidir, de manera libre e informada, sobre el uso de la información que les pertenece, es importante resaltar lo siguiente:

¿Quiénes son el titular y el responsable de los datos personales?

Titular: Persona física a quien corresponden los datos personales.

Responsable: Se entiende por responsable a quien decide sobre el tratamiento de los datos personales, es decir, quien establece las finalidades del tratamiento o el uso que se le dará a los datos personales, el tipo de datos que se requieren, a quién y para qué se comparten, cómo se obtienen, almacenan y suprimen los datos personales, y en qué casos se divulgarán, entre otros factores de decisión.

¿Qué son datos personales y datos personales sensibles?

Se entiende por datos personales: cualquier información concerniente a una persona física identificada o identificable, de manera enunciativa más no limitativa se consideran los siguientes: nombre, domicilio, teléfono móvil, teléfono particular, fotografía, correo electrónico, CURP.

Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

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

¿Qué es el tratamiento de datos personales?

Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con las siguientes acciones:

|  |  |  |
| --- | --- | --- |
| Obtención  Uso  Registro  Organización  Conservación  Elaboración | Utilización  Comunicación  Difusión  Almacenamiento  Posesión  Acceso | Manejo  Aprovechamiento  Divulgación  Transferencia  Disposición |

En ese sentido, el INC, como sujeto Obligado es consciente que el tratamiento de datos personales puede conllevar riesgos si se da un mal uso, una inadecuada gestión o cuidado, que podrían tener consecuencias como daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, en ese sentido, este Instituto, procura que el tratamiento de Datos Personales se realice conforme lo establecido en la legislación aplicable, y bajo los términos que se explican a continuación:

1. **Principios que rigen la Protección de los Datos Personales.**

Licitud: El tratamiento de datos personales por parte del responsable deberá sujetarse a las facultades o atribuciones que la normatividad aplicable le confiera.

Finalidad: Todo tratamiento de datos personales que efectúe el responsable deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable le confiera.

Lealtad: El responsable no deberá obtener y tratar datos personales, a través de medios engañosos o fraudulentos, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad.

Consentimiento: Cuando no se actualicen algunas de las causales de excepción previstas en el artículo 22 de la Ley General, el responsable deberá contar con el consentimiento previo del titular para el tratamiento de los datos personales.

Calidad: El responsable deberá adoptar las medidas necesarias para mantener exactos, completos, pertinentes, correctos y actualizados los datos personales en su posesión, a fin de que no se altere su veracidad. Se presume que se cumple con la calidad en los datos personales cuando éstos son proporcionados directamente por su titular y hasta que éste no manifieste y acredite lo contrario. Cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento, deberán ser suprimidos, previo bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos.

Proporcionalidad: El responsable sólo deberá tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.

Información: El responsable deberá informar al titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.

Responsabilidad: El responsable deberá adoptar políticas e implementar mecanismos para asegurar y acreditar el cumplimiento de los principios, deberes y demás obligaciones establecidas en la Ley General.

1. **Deberes que rigen la Protección de los Datos Personales.**

Los deberes que aplican y que se deben observar para el tratamiento de los datos personales son el de confidencialidad y de seguridad, los cuales se describen a continuación:

*Confidencialidad.*

El responsable debe establecer controles o mecanismos que tengan por objeto que todas aquellas personas que traten datos personales, en cualquier fase del tratamiento mantengan en secreto la información, así como evitar que la información sea revelada a personas no autorizadas y prevenir la divulgación no autorizada de la misma.

Implica la obligación de guardar secreto respecto de los datos personales que son tratados, para evitar causar un daño a su titular.

*Seguridad.*

El responsable del tratamiento de datos personales, debe 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.

* Integridad: es la propiedad de salvaguardar la exactitud y completitud de la información, así como evitar la modificación no autorizada o accidental de la misma.
* Confidencialidad: es la propiedad de la información para no estar a disposición o ser revelada a personas no autorizadas.

1. **Generalidades del ciclo de vida de los Datos Personales**

En el respeto de los principios y el cumplimiento de los deberes previstos para el tratamiento de los datos personales, se deberán considerar las etapas que integran el ciclo de vida de los datos personales, las cuales son:

* Obtención.
* Uso (registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento divulgación, transferencia o disposición); y,
* Eliminación.

Las etapas del ciclo de vida de los datos personales se concatenan con los principios y deberes de la forma que se indica a continuación:

Por tanto, las áreas que dan tratamiento a Datos Personales deberán alinear cada etapa del ciclo de vida de acuerdo al principio y deber respectivo, lo anterior con la intención de dar debido tratamiento a la información que obra en los archivos de cada área.

# V. PROGRAMA GENERAL DE DATOS PERSONALES

El Instituto Nacional de Cardiología Ignacio Chávez, a través del Comité de Transparencia y en conjunto con la Unidad de Transparencia, estableció las acciones que se deberán llevar a cabo para la protección, tratamiento y conservación de los datos personales. Tales acciones, en esencia, constituyen las atribuciones y obligaciones siguientes:

Comité de Transparencia.

* Aprobar las políticas y programas internos de protección de datos personales.
* Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales.
* Supervisar el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad.

Unidad de Transparencia.

* Elaborar las políticas y programas internos de protección de datos personales.
* Establecer un sistema de supervisión de vigilancia para comprobar el cumplimiento de las políticas en materia de datos personales.
* Documentar el Sistema de Gestión de Seguridad y elaborar el documento de seguridad.

Áreas del INC.

* Observar los principios de calidad, consentimiento, finalidad, información, lealtad, licitud, proporcionalidad y responsabilidad.
* Adoptar las medidas necesarias para mantener exactos, completos, pertinentes, correctos y actualizados los datos personales en su posesión.
* Mantener estricto control sobre los datos personales que obren en sus archivos, teniendo prohibido difundir o realizar un uso no autorizado de los datos personales, incluso finalizado el tratamiento.

Considerando lo anterior, y con la finalidad de alcanzar los objetivos planteados en el Sistema de Gestión, las políticas y directrices internas de protección de datos personales resultan de observancia obligatoria para todos los servidores públicos adscritos a este H. Instituto que dan tratamiento a Datos Personales.

# VI. MEDIDAS DE SEGURIDAD

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

* Administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional.
* 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.
* Físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales.

# VII. TRANSFERENCIA DE DATOS PERSONALES

La transferencia es toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado.

Este apartado se refiere a los aspectos que las instancias deberán observar al efectuar una transferencia de datos personales.

* Aspectos Generales

Por transferencia debe entenderse todo traslado de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta de:

1. Su titular.
2. El Instituto Nacional de Cardiología Ignacio Chávez INC.
3. Los encargados contratados por el INC.

De los artículos 65 y 66 de la Ley General se desprenden dos reglas aplicables a las transferencias de datos personales:

1. Toda transferencia de datos personales sea nacional o internacional, se encuentra sujeta al consentimiento de su titular, salvo las excepciones previstas en los artículos 22, 66 y 70 de la Ley General.
2. Toda transferencia debe encontrarse formalizada mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, de conformidad con la normatividad aplicable al INC.

A continuación, se abundará sobre dichas reglas generales y sus excepciones correspondientes.

* El consentimiento del titular de los datos personales ante transferencias.

Toda transferencia de datos personales, sea ésta nacional o internacional, se encuentra sujeta al consentimiento de su titular, salvo las excepciones previstas en los artículos 22, 66 y 70 de la Ley General.

Lo anterior implica que, las instancias deben contar con el consentimiento del titular de los datos personales para realizar transferencias, con excepción de los supuestos siguientes:

* Cuando la transferencia esté prevista en la Ley General u otras leyes, convenios o tratados internacionales suscritos y ratificados por México.
* Cuando la transferencia se realice entre el INC y otro responsable, siempre y cuando los datos personales se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales.
* Cuando la transferencia sea legalmente exigida para la investigación y persecución de los delitos, así como la procuración o administración de justicia.
* Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho ante autoridad competente, siempre y cuando medie el requerimiento de esta última.
* Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria tratamiento médico o la gestión de servicios sanitarios, siempre y cuando dichos fines sean acreditados.
* Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el CJF y el titular de los datos personales.
* Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el CJF y un tercero.
* Cuando se trate de los casos en los que el CJF no está obligado a recabar el consentimiento del titular para el tratamiento y transmisión de sus datos personales, conforme a lo dispuesto en el artículo 22 de la Ley General.
* Cuando la transferencia sea necesaria por razones de seguridad nacional.

Bajo el esquema expuesto, si la transferencia a realizar se encuentra sujeta al consentimiento del titular de los datos personales, las instancias deberán realizar las gestiones necesarias para recabarlo.

Al respecto, de conformidad con el artículo 113 de los Lineamientos Generales, por regla general el consentimiento a que se refiere el punto anterior será tácito, salvo que una ley exija al INC recabar el consentimiento expreso para la transferencia de sus datos personales.

En términos de lo previsto en el artículo 114 de los citados Lineamientos, cuando se requiera el consentimiento expreso, la instancia podrá establecer cualquier medio lícito que le permita obtenerlo de manera previa a la transferencia de los datos personales.

En todos los casos, las instancias deberán verificar que en el aviso de privacidad correspondiente al tratamiento en que los datos personales fueron recabados, se realice lo siguiente:

* Se informe al titular de la transferencia a realizar.
* Los mecanismos y medios disponibles para que el titular, en su caso, pueda manifestar su negativa para el tratamiento de sus datos personales para finalidades y transferencias de datos personales que requieren su consentimiento, de conformidad con el artículo 27, fracción IV, de la Ley General.

En términos del artículo 113 de los Lineamientos Generales, el INC deberá comunicar al destinatario o receptor de los datos personales el aviso de privacidad conforme al cual se obligó a tratar los datos personales frente al titular.

* Formalización de la transferencia.

De conformidad con el artículo 66 de la Ley General, toda transferencia deberá formalizarse mediante alguno de los medios siguientes:

* Suscripción de cláusulas contractuales.
* Convenios de colaboración.
* Instrumentos jurídicos que de conformidad con la normatividad que resulte aplicable, permitan demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes.

Dicha formalización no será aplicable en los casos siguientes:

* Cuando la transferencia sea nacional y se realice entre responsables en virtud del cumplimiento de una disposición legal o en el ejercicio de atribuciones expresamente conferidas a éstos.
* Cuando la transferencia sea internacional y se encuentre prevista en una ley o tratado suscrito y ratificado por México, o bien, se realice a petición de una autoridad extranjera u organismo internacional competente en su carácter de receptor, siempre y cuando las facultades entre el responsable transferente y receptor sean homólogas, o bien, las finalidades que motivan la transferencia sean análogas o compatibles respecto de aquéllas que dieron origen al tratamiento del responsable transferente

En ese orden de ideas, si la transferencia no se ubica en ninguno de las excepciones referidas, previo a la realización de una transferencia de datos personales, las instancias deberán realizar lo siguiente:

|  |
| --- |
| ACTIVIDADES A REALIZAR ANTE TRANSFERENCIA DE DATOS PERSONALES |
| Identificar las cláusulas contractuales, convenios de colaboración o instrumentos jurídicos existentes en que se encuentren previstas las transferencias de los datos personales. |
| Verificar que, en dichas cláusulas contractuales, convenios o instrumentos, se refleje el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes. |
| Comunicar al tercero receptor el aviso de privacidad correspondiente al tratamiento en que se obtuvieron los datos personales. |
| Solicitar al tercero receptor que manifieste por escrito que se obliga a proteger los datos personales conforme a los principios y deberes que establece la Ley General y las disposiciones que resulten aplicables en la materia. |

# VIII. REMISIÓN DE DATOS PERSONALES

La remisión se refiere a toda comunicación de datos personales realizada exclusivamente entre el INC y una persona ajena que sola o conjuntamente con otras, efectuará el tratamiento datos personales a nombre y por cuenta del propio INC.

Para efectos de la remisión de datos personales, la persona ajena que sola o conjuntamente con otras efectúe el tratamiento, se le denomina encargado*.*

En mérito de lo anterior de conformidad con los artículos 59 a 62 de la Ley General y 108 a 110 de los Lineamientos Generales, l todas las instancias que, en el ámbito de su competencia, realicen contrataciones que impliquen el tratamiento de datos personales por parte de encargados, deberán formalizar tales relaciones mediante un contrato o instrumento jurídico que contenga las obligaciones y cláusulas antes señaladas, incluyendo aquella que regule lo que procederá en caso de que el encargado desee subcontratar servicios que involucren el tratamiento de datos personales

Dicho contrato o instrumento deberá considerar con carga al encargado, al menos, las obligaciones siguientes:

|  |
| --- |
| OBLIGACIONES DE LA REMISION DE DATOS PERSONALES |
| Realizar el tratamiento de los datos personales conforme a la normativa del INC y a las instrucciones que, en su caso, se indiquen en el contrato o instrumento jurídico respectivo. |
| Implementar medidas de seguridad conforme a la Ley General, Lineamientos Generales, Acuerdo General y los instrumentos jurídicos aplicables. |
| Abstenerse de tratar los datos personales para finalidades distintas a las establecidas en la normativa del INC o de lo instruido en el contrato o instrumento jurídico respectivo. |
| Abstenerse de tratar los datos personales para finalidades distintas a las establecidas en la normativa del INC o de lo instruido en el contrato o instrumento jurídico respectivo. |
| Implementar medidas de seguridad conforme a la Ley General, Lineamientos Generales, Acuerdo General y los instrumentos jurídicos aplicables |
| Informar inmediatamente sobre la vulneración de datos personales a la instancia del INC |
| Guardar la confidencialidad respecto de los datos personales |
| Generar, actualizar y conservar la documentación necesaria que le permita acreditar el cumplimiento de todas las obligaciones. |
| Permitir y colaborar con el INC o con el INAI, para realizar verificaciones en el lugar o establecimiento donde se lleva a cabo el tratamiento de los datos personales, o en su caso, proporcionar la documentación o información que se estime necesaria. |
| Suprimir o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el INC, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. |

* Regulación de subcontrataciones en la remisión de datos personales.

El contrato o instrumento jurídico en que se convenga la remisión, deberá incluir la regulación procedente en caso de que el encargado desee subcontratar servicios que involucren el tratamiento de los datos personales.

En todos los casos, las instancias competentes deberán conocer y autorizar las subcontrataciones que el encargado realice.

Las autorizaciones se podrán otorgar desde el contrato original, cuando el encargado ya prevea subcontrataciones específicas y garantice que las mismas se realizarán en las condiciones precisadas. En caso contrario, la autorización se podrá realizar de manera posterior.

Asimismo, se deberá comunicar al encargado que el contrato o el instrumento jurídico mediante el cual se formalice la subcontratación deberá incluir cláusulas con las obligaciones indicadas.

# IX. EJERCICIO DE LOS DERECHOS ARCO

Este apartado se refiere a los aspectos que las instancias deberán considerar ante el ejercicio de los derechos de acceso, rectificación, cancelación y oposición de datos personales.

A

R

O

C

# X. CÓMPUTO EN LA NUBE

Cómputo en la nube, se refiere a un 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.

En términos de los artículos 63 y 64 de la Ley General, el INC podrá contratar o adherirse a servicios, aplicaciones e infraestructura de cómputo en la nube, y otras materias que impliquen el tratamiento de datos personales, siempre y cuando el proveedor externo garantice las políticas de protección de datos personales equivalentes a los principios, deberes, obligaciones y responsabilidades establecidas en la Ley General, los Lineamientos Generales, el Acuerdo General y demás disposiciones que resulten aplicables en la materia.

En caso de que el INC contrate dichos servicios, deberá delimitar el tratamiento de los datos personales por parte del proveedor externo a través de cláusulas contractuales u otros instrumentos jurídicos.

Por otro lado, en el supuesto de que el INC se adhiera a dichos servicios mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente:

* Tener y aplicar políticas de protección de datos personales afines a los principios y deberes que establecen la Ley General, los Lineamientos Generales, el Acuerdo General y demás normativa aplicable.
* Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio.
* Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que preste el servicio.
* Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.

Aparte de lo anteriormente mencionado, se deberá verificar que el proveedor cuente con mecanismos, al menos, para:

* Establecer y mantener medidas de seguridad para la protección de los datos personales sobre los que se preste el servicio
* Impedir el acceso a los datos personales a personas que no cuenten con permisos de acceso, o bien, en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al INC.
* Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al INC y que este último haya podido recuperarlos.

Por ningún motivo, el INC podrá adherirse a servicios que no garanticen la debida protección de los datos personales, conforme a la Ley General, Lineamientos Generales, Acuerdo General y demás disposiciones que resulten aplicables en la materia.

Es importante referir que, de conformidad con lo estipulado en el artículo 111 de los Lineamientos Generales, los proveedores de servicios de cómputo en la nube tendrán el carácter de encargados, por lo que la instancia que pretenda contratar sus servicios deberá verificar el cumplimiento de lo estipulado en el capítulo de este programa denominado “Remisión de datos personales”; es decir, además de observar las obligaciones señaladas, deberá incluir en el contrato o instrumento jurídico las obligaciones generales de cualquier encargado, las cuales son:

* Realizar el tratamiento de los datos personales conforme a la normativa del INC y a las instrucciones que, en su caso, se indiquen en el contrato o instrumento jurídico respectivo.
* No tratar los datos personales para finalidades distintas a las establecidas en la normativa del INC y de lo instruido en el contrato o instrumento jurídico respectivo.
* Implementar medidas de seguridad para la protección de los datos personales.
* Guardar confidencialidad respecto de los datos personales tratados.

# XI. PORTABILIDAD DE DATOS PERSONALES

La portabilidad constituye un derecho de los titulares que tiene por objeto la reutilización de sus datos personales.

A través del ejercicio de la portabilidad, los titulares pueden recibir los datos personales que han proporcionado a un responsable y transmitirlos a otro responsable, siempre y cuando los datos personales se encuentren en un formato estructurado, de uso común y lectura mecánica.

En términos de lo previsto en el artículo 57 de la Ley General, el titular podrá ejercer el derecho de portabilidad cuando el tratamiento de los datos personales cuente con las características siguientes:

1. Se realice vía electrónica;
2. Tenga un formato estructurado y comúnmente utilizado; y
3. El titular hubiere proporcionado directamente al CJF sus datos personales de forma activa y consciente

Cuando se actualicen los supuestos, el titular tendrá derecho a transmitir sus datos personales y cualquier otra información que haya facilitado y que se conserve en un sistema de tratamiento automatizado, a otro sistema en un formato electrónico comúnmente utilizado, sin impedimentos por parte del responsable del tratamiento de quien se retiren los datos personales.

* Tramite del ejercicio de Portabilidad.

De conformidad con el artículo 14 de los Lineamientos para la Portabilidad, en relación con los numerales 51, 52, octavo párrafo de la Ley General, y 27, fracción I, de dichos lineamientos, la atención de las solicitudes de portabilidad de los datos personales se realizará a través de la Unidad de Transparencia del INC.

# XII. CICLO DE VIDA DE LOS DATOS PERSONALES

A fin de mantener las medidas de seguridad para la protección de los datos personales, se deberán crear políticas internas para su gestión y tratamiento que consideren el contexto en el que ocurren los tratamientos, así como el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior eliminación.

El diseño e implementación de las políticas internas para la gestión y el tratamiento de los datos personales, se deberá incluir la identificación del ciclo de vida de los datos personales respecto de cada tratamiento que se efectúe; considerando su:

Para definir el ciclo de vida de los datos personales, se deberá partir de las etapas que se representan en el esquema siguiente:

# XIII. EVALUACIÓN EN LA PROTECCIÓN DE DATOS PERSONALES

En términos del artículo 74 de la Ley General, cuando se pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que a su juicio implique el tratamiento intensivo o relevante de datos personales, se deberá realizar una evaluación de impacto en la protección de datos personales, y presentarla ante el INAI, quien podrá emitir recomendaciones no vinculantes especializadas en la materia de protección de datos personales.

* Aspectos Generales.

Cuando se pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que a su juicio implique el tratamiento intensivo o relevante de datos personales, se deberá realizar una evaluación de impacto en la protección de datos personales, y presentarla ante el INAI, quien podrá emitir recomendaciones no vinculantes especializadas en la materia de protección de datos personales.

Se estará en presencia de un tratamiento intensivo o relevante de datos personales cuando ocurra alguna de las condiciones siguientes:

* Eva**lu**ación de Impacto.

Consiste en la valoración de las consecuencias 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

Las instancias que pretendan implementar o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que a su juicio implique el tratamiento intensivo o relevante de datos personales, 45 días hábiles previos a la fecha en que se considere poner en operación, deberán emitir un informe dirigido a la Unidad de Transparencia que dé cuenta de los aspectos siguientes:

Una vez recibido el informe, la Unidad de Transparencia analizará que el tratamiento de datos personales efectivamente actualice los supuestos de un tratamiento intensivo o relevante en términos de lo previsto en la Ley General y los Lineamientos para la Evaluación de Impacto, lo que deberá hacer del conocimiento del Comité de Transparencia.

En caso de que se verifique que el supuesto constituye un tratamiento intensivo o relevante, se deberá realizar una evaluación de impacto en la protección de datos personales, y presentarla ante el INAI con un mínimo de 30 días hábiles previos a la fecha en que se pretenda poner en operación o modificar el tratamiento respectivo.

# XIV. CAPACITACIÓN DE LOS SERVIDORES PÚBLICOS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

El programa anual de capacitación del INCAR tiene por objetivo la capacitación de sus servidores públicos, por lo tanto busca continuar con la capacitación de su personal en materia de protección y tratamiento de datos personales, en ese sentido, el Área de Prestaciones y Capacitación de la Subdirección de Administración y Desarrollo de Personal, se encarga de identificar los requerimientos de capacitación, es decir, los conocimientos, habilidades y actitudes de los servidores públicos del INCAR, lo anterior, lo realiza a través de una cédula de detección de necesidades de capacitación remitida a las unidades administrativas, contando así con una herramienta que da cuenta de un diagnóstico de la demanda en la formación en la materia.

La capacitación de personal dentro del Instituto se realiza a través de conferencias y pláticas informativas que pueden ser de manera presencial o en línea, el enlace de capacitación es el encargado de remitir vía electrónica los cursos que imparte el INAI, para que el personal se inscriba a los cursos que sean de su interés.

El programa anual de capacitación en materia de protección de datos personales se puede consultar en la siguiente liga electrónica <https://www.cardiologia.org.mx/transparencia/proteccion_de_datos_personales/index.php> .