SENER
SECRETARÍA DE ENERGÍA

ININ
INSTITUTO NACIONAL DE INVESTIGACIONES NUCLEARES

DOCUMENTO DE SEGURIDAD

Versión 08 de diciembre de 2023

SENER
SECRETARÍA DE ENERGÍA

INSTITUTO NACIONAL DE INVESTIGACIONES NUCLEARES

Contenido

Introducción

El 26 de enero de 2017 se expidió la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (en lo sucesivo, la Ley General de Datos), la cual tiene como objetivo establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales que estén en posesión de los sujetos obligados.

En su artículo primero, la Ley General de Datos señala 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 ese sentido, el Instituto Nacional de Investigaciones Nucleares (ININ o Instituto) al ser un organismo público descentralizado del gobierno federal, es sujeto obligado de la Ley General de Datos y, por ello, debe observar lo dispuesto por dicho instrumento normativo en el tratamiento de datos personales que lleve a cabo.

De acuerdo con lo dispuesto por Ley General de Datos, el tratamiento de datos personales que realicen los sujetos obligados estará regido por ocho principios y dos deberes. Los ocho principios son: licitud, lealtad, información, consentimiento, finalidad, proporcionalidad, calidad y responsabilidad; mientras que los dos deberes son el de confidencialidad y seguridad. Estos principios, deberes y derechos imponen una serie de obligaciones para los sujetos regulados por la Ley General de Datos, cuya finalidad es que el tratamiento se realice garantizando la protección de los datos personales, con el objeto de respetar el derecho a la autodeterminación informativa de los titulares.

Asimismo, la Ley General de Datos detalla el alcance y los procedimientos para el ejercicio de los cuatro derechos que el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos reconoce a los titulares de los datos personales: acceso, rectificación, cancelación y oposición (derechos ARCO), y reconoce uno más, el de portabilidad.

En específico, con relación al deber de seguridad, el artículo 31 de la Ley General de Datos señala que el responsable del tratamiento deberá establecer y mantener 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.

Al respecto, el artículo 33 de la Ley General de Datos señala lo siguiente:

> ***Artículo 33.*** *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.*

Por su parte, el artículo 35 de la Ley General de Datos establece como una obligación la elaboración de un documento de seguridad, que se define -según la fracción XIV del artículo 3 de la Ley General de Datos- como el 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.

De conformidad con el artículo 35 de la Ley General de Datos, el documento deberá contener, al menos, la siguiente información:

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.

Asimismo, de conformidad con los artículos 83 y 84 del Título Séptimo de la Ley General de Datos, denominado Responsables en Materia de Protección de Datos Personales en Posesión de los Sujetos Obligados, se cuenta con un Comité integrado y con las funciones dispuestas en la Ley General de Transparencia y Acceso a la Información Pública y demás normatividad aplicable, como se expresa a continuación:

Capítulo I
Comité de Transparencia

Artículo 83. *Cada responsable contará con un Comité de Transparencia, el cual se integrará y funcionará conforme a lo dispuesto en la Ley General de Transparencia y Acceso a la Información Pública y demás normativa aplicable.*

El Comité de Transparencia será la autoridad máxima en materia de protección de datos personales.

Artículo 84. *Para los efectos de la presente Ley y sin perjuicio de otras atribuciones que le sean conferidas en la normatividad que le resulte aplicable, el Comité de Transparencia tendrá las siguientes funciones:*

I. *Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, de conformidad con las disposiciones previstas en la presente Ley y en aquellas disposiciones que resulten aplicables en la materia;*
II. *Instituir, en su caso, procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO;*
III. *Confirmar, modificar o revocar las determinaciones en las que se declare la inexistencia de los datos personales, o se niegue por cualquier causa el ejercicio de alguno de los derechos ARCO;*
IV. *Establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor observancia de la presente Ley y en aquellas disposiciones que resulten aplicables en la materia;*
V. *Supervisar, en coordinación con las áreas o unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad;*
VI. *Dar seguimiento y cumplimiento a las resoluciones emitidas por el Instituto y los organismos garantes, según corresponda;*
VII. *Establecer programas de capacitación y actualización para los servidores públicos en materia de protección de datos personales, y*
VIII. *Dar vista al órgano interno de control o instancia equivalente en aquellos casos en que tenga conocimiento, en el ejercicio de sus atribuciones, de una presunta*

irregularidad respecto de determinado tratamiento de datos personales; particularmente en casos relacionados con la declaración de inexistencia que realicen los responsables.

Por su parte, el artículo 85 de la Ley General de Datos establece que los Responsables tendrán una Unidad de Transparencia (UT), que se integrará y funcionará conforme a lo dispuesto en la Ley General de Transparencia y Acceso a la Información Pública y demás normatividad aplicable, que, para efectos del tratamiento de datos personales, tendrá las siguientes funciones:

Capítulo II
De la Unidad de Transparencia

Artículo 85. *Cada responsable contará con una Unidad de Transparencia, se integrará y funcionará conforme a lo dispuesto en la Ley General de Transparencia y Acceso a la Información Pública, esta Ley y demás normativa aplicable, que tendrá las siguientes funciones:*

I. Auxiliar y orientar al titular que lo requiera con relación al ejercicio del derecho a la protección de datos personales;
II. Gestionar las solicitudes para el ejercicio de los derechos ARCO;
III. Establecer mecanismos para asegurar que los datos personales solo se entreguen a su titular o su representante debidamente acreditados;
IV. Informar al titular o su representante el monto de los costos a cubrir por la reproducción y envío de los datos personales, con base en lo establecido en las disposiciones normativas aplicables;
V. Proponer al Comité de Transparencia los procedimientos internos que aseguren y fortalezcan mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO;
VI. Aplicar instrumentos de evaluación de calidad sobre la gestión de las solicitudes para el ejercicio de los derechos ARCO, y
VII. Asesorar a las áreas adscritas al responsable en materia de protección de datos personales.

En ese sentido, en cumplimiento de las obligaciones antes descritas, a continuación, se presenta el Documento de Seguridad del ININ con los elementos informativos que establece el artículo 35 de la Ley General de Datos.

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

El artículo 33, fracción I de la Ley General de Datos establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, la elaboración de un inventario de datos personales y de los sistemas de tratamiento.

Como se señaló, de acuerdo con la fracción I del artículo 35 de la Ley General de Datos, este inventario forma parte del documento de seguridad.

Sobre el particular, los artículos 58 y 59 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público (en adelante, Lineamientos Generales), 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*

VI. *La cancelación, supresión o destrucción de los datos personales.*

El responsable deberá identificar el riesgo inherente de los datos personales, contemplando su ciclo de vida y los activos involucrados en su tratamiento, como podrían ser hardware, software, personal, o cualquier otro recurso humano o material que resulte pertinente considerar.

A partir de lo anterior, el ININ elaboró los inventarios de los distintos tratamientos de datos personales que realiza, identificando los elementos informativos que señala el artículo 58 de los Lineamientos Generales y basados en el ciclo de vida de los datos personales, como lo requiere el artículo 59 de los Lineamientos Generales.

Los inventarios forman parte integral del presente documento de seguridad y se encuentran contenidos en el **Anexo 1.**

Con independencia de lo anterior, el siguiente cuadro muestra un resumen de los inventarios elaborados:

	Adscripción	Área	Siglas	Clave de Inventario	Denominación del Inventario de Tratamiento de Datos Personales
1	Gerencia de Recursos Humanos	Departamento de Administración y Capacitación de Personal	DACP	**DS-2023-DACP-1**	Sistema de Nómina
2		Departamento de Administración y Capacitación de Personal	DACP	**DS-2023-DACP-2**	Sistema de Control de Asistencia
3		Departamento de Administración y Capacitación de Personal	DACP	**DS-2023-DACP-3**	Sistema de Liquidaciones
4		Departamento de Administración y Capacitación de Personal	DACP	**DS-2023-DACP-4**	Sistema de Liquidaciones

	Adscripción	Área	Siglas	Clave de Inventario	Denominación del Inventario de Tratamiento de Datos Personales
5		Departamento de Administración y Capacitación de Personal	DACP	**DS-2023-DACP-5**	Sistema de Datos Generales
6		Departamento de Administración y Capacitación de Personal	DACP	**DS-2023-DACP-6**	Sistema de Control de Plazas
7	Gerencia de Sistemas	Gerencia de Sistemas	GS	**DS-2024-GS-7**	Padrón Electrónico de Becarios

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

El artículo 33, fracción II de la Ley General de Datos establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, la definición de las funciones y obligaciones del personal involucrado en el tratamiento de datos personales.

Como se señaló, de acuerdo con la fracción II del artículo 35 de la Ley General de Datos, este elemento informativo forma parte del documento de seguridad.

Sobre el particular, el artículo 57 de los Lineamientos Generales señala 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.*

De conformidad con lo anterior, las funciones y obligaciones del personal del ININ que trata datos personales se han identificado a través de los inventarios que se desarrollaron por cada uno de los tratamientos, en los cuales se identificó el personal que realiza el tratamiento, el área al que está adscrito y la finalidad de dicho tratamiento.

En este sentido, el inventario de tratamientos contiene las siguientes columnas, en las cuales se identifican las funciones del personal que interviene en el tratamiento de los datos personales:

Sistema de Datos Personales	***Persona Servidora Pública que tienen acceso al Sistema de Datos Personales***	***Área de Adscripción***	***Finalidad del acceso***
Indicar la denominación del Sistema de Datos Personales	*Señalar los puestos de las personas servidoras públicas que tienen acceso a la base de datos del Sistema de Datos Personales. Uno por fila.*	*Definir la unidad administrativa a la que está adscrito el puesto.*	*Señalar con qué fines tienen acceso las personas servidoras públicas identificadas. Una por fila, según corresponda.*

Adicionalmente, conviene señalar que las funciones y obligaciones del personal que traten datos personales se encuentran definidas en la legislación y normatividad que rige el actuar del ININ, por lo cual, para efectos del presente documento de seguridad, el marco normativo de referencia se encuentra establecido en: el Estatuto Orgánico del ININ, el Manual General de Organización del ININ, el Catálogo de Puestos del Personal Sindicalizado, así como en el Catálogo y Perfil de Puestos del Personal Operativo de Confianza (**Anexo 2**).

Asimismo, la Gerencia de Sistemas (GS), adscrita a la Dirección de Servicios Tecnológicos, emitió las Directivas de Seguridad de la Información del Instituto Nacional de Investigaciones Nucleares (**Anexo 3**), siendo la responsable de definir los documentos normativos derivados de las mismas en conjunto con las áreas involucradas, tales como: normas, procedimientos y lineamientos específicos, así como de administrar, implementar y mantener medidas de control, supervisión y vigilancia de acceso a los activos de información de acuerdo a las necesidades que se presenten en el ININ y en apego al *ACUERDO por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal*, publicado el 6 de septiembre de 2021, entre otros marcos normativos relacionados con la materia; ello, en apego al Artículo 29 del Estatuto Orgánico del Instituto Nacional de Investigaciones Nucleares, publicado el 28 de septiembre de 2010, en el Diario Oficial de la Federación.

Estas Directivas de Seguridad de la Información del Instituto Nacional de Investigaciones Nucleares se deben aplicar independientemente de la manera en que se presenta la información (impresa, oral, electrónica y/o visual), la tecnología usada para manipular la información, la ubicación de la información o la clasificación de esta y serán de obligatorio cumplimiento para el personal del ININ.

Asimismo, será responsabilidad de los niveles de supervisión ejecutar y hacer cumplir estas disposiciones regulatorias ya que su definición y aprobación por sí sola no constituye una garantía en materia de Seguridad de la Información del Instituto.

III, IV y V. Análisis de riesgos, análisis de brecha y Plan de Trabajo.

El artículo 33, fracciones IV, V y VI de la Ley General de Datos establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, la realización del análisis de riesgo, análisis de brecha y plan de trabajo, en los siguientes términos:

> ***Artículo 33.*** *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.*** *[…]*
> ***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;*
> *[…]*

Como se señaló, de acuerdo con las fracciones III, IV y V del artículo 35 de la Ley General de Datos, los análisis de riesgo y brecha y el plan de trabajo forman parte del documento de seguridad.

Por su parte, los artículos 60, 61 y 62 de los Lineamientos Generales establecen lo siguiente:

> ***Análisis de riesgos***
> ***Artículo 60.*** *Para dar cumplimiento al artículo 33, fracción IV de la Ley General, el responsable deberá realizar un análisis de riesgos de los datos personales tratados considerando lo siguiente:*
>
> ***I.*** *Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico;*

II. El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida;
III. El valor y exposición de los activos involucrados en el tratamiento de los datos personales;
IV. Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida, y
V. Los factores previstos en el artículo 32 de la Ley General.

Análisis de brecha
Artículo 61. *Con relación al artículo 33, fracción V de la Ley General, para la realización del análisis de brecha el responsable deberá considerar lo siguiente:*

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

Plan de trabajo
Artículo 62. *De conformidad con lo dispuesto en el artículo 33, fracción VI de la Ley General, el responsable deberá elaborar un plan de trabajo que defina las acciones a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer.*

Lo anterior, considerando los recursos designados; el personal interno y externo en su organización y las fechas compromiso para la implementación de las medidas de seguridad nuevas o faltantes.

Por su parte, el artículo 32 de la Ley General de Datos, citado en la fracción V del artículo 60 de los Lineamientos Generales, dispone lo siguiente:

Artículo 32. *Las medidas de seguridad adoptadas por el responsable deberán considerar:*

I. El riesgo inherente a los datos personales tratados;
II. La sensibilidad de los datos personales tratados;
III. El desarrollo tecnológico;
IV. Las posibles consecuencias de una vulneración para los titulares;
V. Las transferencias de datos personales que se realicen;
VI. El número de titulares;
VII. Las vulneraciones previas ocurridas en los sistemas de tratamiento, y
VIII. 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.

A partir de lo dispuesto por los artículos antes citados, el análisis de riesgo se lleva a cabo a partir de cuatro fuentes de información:

1. Análisis de riesgos de la infraestructura tecnológica y recursos de software y hardware;
2. Análisis de riesgos de hábitos de seguridad del personal del ININ;
3. Análisis de riesgos a partir de los inventarios de tratamientos de datos personales, y
4. Análisis de riesgos vinculado con el cumplimiento de obligaciones normativas en materia de datos personales.

Los dos primeros análisis se realizan de manera general y aplican transversalmente, ya que el primero refiere a los distintos sistemas o medios en los que se llevan a cabo los diversos tratamientos que realiza el Instituto, por lo que los riesgos y controles que se determinen aplican de manera directa a estos medios o sistemas; mientras que el segundo versa sobre los hábitos de seguridad del personal, de manera general y no asociados a un tratamiento en lo particular.

Por su parte, los análisis 3 y 4 se realizan, de manera específica, asociados a cada uno de los tratamientos, y tomando en cuenta sus particularidades.

De igual forma, se ha realizado la estimación de las vulnerabilidades y amenazas que impactan a los tratamientos reportados en los inventarios contenidos en el Anexo 1, así como el nivel de riesgo que esto representa, el cual se determinó con base en el tipo de datos personales, su riesgo inherente y el nivel de seguridad requerido, tal y como se muestra a continuación:

a) Datos personales con riesgo inherente bajo: Considera datos de identificación y contacto o información laboral o académica, tal como nombre, teléfono particular, edad, sexo, Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), estado civil, correo electrónico, lugar y fecha de nacimiento, nacionalidad, puesto de trabajo y lugar de trabajo, idioma o lengua, escolaridad, cédula profesional, información migratoria, entre otros que no se encuentran en los incisos b) y c).

b) Datos personales con riesgo inherente medio: Contempla los datos que permiten conocer la ubicación física de la persona, tales como la dirección física, información relativa al tránsito de las personas dentro y fuera del país, y/o cualquier otro que permita volver identificable a una persona a través de los datos que proporcione alguien más. Por ejemplo: dependientes, beneficiarios, familiares, referencias laborales, referencias personales, etc.

También son datos de riesgo inherente medio aquéllos que permitan inferir el patrimonio de una persona, que incluya entre otros, los saldos bancarios, estados y/o número de cuenta, cuentas de inversión, bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos, egresos, buró de crédito, seguros, afores, fianzas, sueldos y salarios, servicios contratados. Incluye el número de tarjeta bancaria de crédito y/o débito. Son considerados también los datos de autenticación con información referente a los usuarios, contraseñas, información biométrica (huellas dactilares, iris, voz, entre otros), firma autógrafa y electrónica, fotografías, identificaciones oficiales, inclusive escaneadas o fotocopiadas y cualquier otro que permita autenticar a una persona. Dentro de esta categoría se toman en cuenta los datos jurídicos tales como antecedentes penales, amparos, demandas, contratos, litigios y cualquier otro tipo de información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa.

c) Datos con riesgo inherente alto: Se refiere a los datos personales sensibles, que de acuerdo a la Ley General de Datos, incluyen datos de salud, los cuales se refieren a la información médica donde se documente el estado de salud física y mental, pasado, presente o futuro; información genética; origen racial o étnico; ideología, creencias religiosas, filosóficas y morales; afiliación sindical, opiniones políticas; preferencia sexual, hábitos sexuales y cualquier otro cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para el titular.

Por lo anterior, para determinar el nivel de riesgo las unidades administrativas considerarán el criterio de riesgo inherente del dato personal, así como el nivel de seguridad requerido para éste, en adición a las vulnerabilidades y amenazas, conforme a lo siguiente:

Criterios del Nivel de Riesgo	
Riesgo inherente bajo	**Nivel de seguridad bajo**
Riesgo inherente medio	**Nivel de seguridad medio**
Riesgo inherente alto	**Nivel de seguridad alto**

Los elementos requeridos en los artículos 33, fracción IV, de la Ley General de Datos y 60 de los Lineamientos Generales se atienden de la siguiente forma:

Elemento requerido	Fundamento	Fuente	Observaciones
Tomar en cuenta amenazas y vulnerabilidades existentes.	33, fracción IV, de la Ley General de Datos.	➢ Análisis de riesgos de la infraestructura tecnológica y recursos de software y hardware.	En los cuatro cuestionarios o fuentes se identifican las vulnerabilidades y amenazas específicas.

Elemento requerido	Fundamento	Fuente	Observaciones
		➢ Análisis de riesgos de hábitos de seguridad del personal del ININ. ➢ Análisis de riesgos de vulneraciones. ➢ Análisis de riesgos vinculado con el cumplimiento de obligaciones normativas en materia de datos personales.	
Tomar en cuenta los recursos involucrados.	33, fracción IV, de la Ley General de Datos.	➢ Análisis de riesgos de la infraestructura tecnológica y recursos de software y hardware. ➢ Análisis de riesgos de vulneraciones.	La primera fuente refiere específicamente a los recursos de software y hardware, mientras que en la segunda, en los inventarios se identifican los medios de almacenamiento y obtención de los datos personales y, en su caso, se asocian con sus respectivos riesgos.
Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico.	60, fracción I, de los Lineamientos Generales.	➢ Análisis de riesgos vinculado con el cumplimiento de obligaciones normativas en materia de datos personales.	El cuestionario respectivo refiere a los requerimientos regulatorios.
El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida.	60, fracción II, de los Lineamientos Generales.	➢ Análisis de riesgos de vulneraciones.	En el inventario se identifica el tipo de datos tratado y se estructura a partir de su ciclo de vida, lo que es considerado al momento de determinar riesgos y controles de seguridad.
El valor y exposición de los activos involucrados en el tratamiento de los datos personales	60, fracción III, de los Lineamientos Generales.	➢ Análisis de riesgos de hábitos de seguridad del personal del ININ.	A través de este cuestionario se identifican las prácticas que exponen a los datos personales.
Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida.	60, fracción IV, de los Lineamientos Generales.	➢ Ponderación de riesgos.	En la ponderación de riesgos que se realiza en la Fase Cuatro se toma en cuenta las posibles consecuencias de una vulneración para los titulares, para la priorización y determinación del tratamiento del riesgo.

Elemento requerido	Fundamento	Fuente	Observaciones
El riesgo inherente a los datos personales tratados.	32, fracción I, de la Ley General de Datos.	➢ Análisis de riesgos de vulneraciones.	En el inventario se identifica el tipo de datos tratado y las finalidades del tratamiento, lo que es considerado al momento de determinar riesgos y controles de seguridad.
La sensibilidad de los datos personales tratados.	32, fracción II, de la Ley General de Datos.	➢ Análisis de riesgos de vulneraciones.	En el inventario se identifica el tipo de datos tratado, lo que es considerado al momento de determinar riesgos y controles de seguridad.
El desarrollo tecnológico.	32, fracción III, de la Ley General de Datos.	➢ Análisis de riesgos de la infraestructura tecnológica y recursos de software y hardware.	En el análisis realizado por la GS se considera el desarrollo tecnológico, ya que versa sobre dicha materia.
Las posibles consecuencias de una vulneración para los titulares.	32, fracción IV, de la Ley General de Datos.	➢ Ponderación de riesgos.	En la ponderación de riesgos que se realiza en la Fase Cuatro se toma en cuenta las posibles consecuencias de una vulneración para los titulares, para la priorización y determinación del tratamiento del riesgo.
Las transferencias de datos personales que se realicen.	32, fracción V, de la Ley General de Datos.	➢ Análisis de riesgos de vulneraciones.	En el inventario se identifican las transferencias, lo que es considerado al momento de determinar riesgos y controles de seguridad.
El número de titulares.	32, fracción VI, de la Ley General de Datos.	➢ Ponderación de riesgos.	En la ponderación de riesgos que se realiza en la Fase Cuatro se toma en cuenta el número de titulares para la priorización y determinación del tratamiento del riesgo.
Las vulneraciones previas ocurridas en los sistemas de tratamiento.	32, fracción VII, de la Ley General de Datos.	➢ Reportes de vulneraciones al Comité de Transparencia.	
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.	32, fracción VIII, de la Ley General de Datos.	➢ Ponderación de riesgos.	En la ponderación de riesgos que se realiza en la Fase Cuatro se toma en cuenta el riesgo por el valor potencial cuantitativo o cualitativo que pudieran tenerlos datos personales tratados para una tercera persona no autorizada para su posesión, para la priorización y determinación del tratamiento del riesgo.

Existen enormes retos a los que se enfrentan todas las instituciones, tanto públicas como privadas, uno de ellos es prever y evitar lo inesperado, especialmente en un escenario que involucra las constantes y novedosas tecnologías de la información.

Por tal motivo, la Ley General de Datos establece la necesidad de contar con un análisis de los riesgos a los cuales se puede enfrentar el tratamiento de los datos personales durante su ciclo de vida. Es así que, en el documento denominado *Recomendaciones para el Manejo de Incidentes de Seguridad de Datos Personales*, emitido por el INAI, se indican los más comunes:

1. Robo de información en documentos y medios de almacenamiento desechados incorrectamente.
2. Empleados que acceden a datos personales sin la autorización correspondiente.
3. Empleados que revelan información a otras personas a través de engaños.
4. Robo o pérdida de equipos de cómputo, laptops, teléfonos inteligentes, tabletas o memorias extraíbles con información personal.
5. Acceso ilegal a las bases de datos personales por un externo.

El proceso de análisis de riesgos, en lo general, es el siguiente:

Fase Uno. Identificación de posibles riesgos y controles de seguridad preliminares.

1) Cada una de las unidades administrativas a cargo de tratamientos de datos personales, responderán los cuestionarios relativos a los análisis de riesgos de hábitos de seguridad y de cumplimiento de obligaciones normativas (**Anexo 4**).

Se atenderá a un único formato de cuestionario de cumplimiento de obligaciones por tratamiento, todo el personal que esté involucrado con el tratamiento debe responder un cuestionario sobre sus hábitos de seguridad.

Una vez respondidos los cuestionarios, la unidad administrativa a cargo de tratamiento de datos personales analizará la respuesta para detectar posibles vulnerabilidades y amenazas a efecto de definir controles de seguridad preliminares.

2) La unidad administrativa a cargo de tratamiento de datos personales analizará los inventarios de datos personales y, en caso de detectar posibles vulnerabilidades y amenazas, definirá controles de seguridad preliminares.

3) La Gerencia de Sistemas realizará el análisis de riesgos de la infraestructura y recursos impresos o electrónicos, de acuerdo con la metodología que tiene definida.

Fase Dos. Entrevistas y determinación de riesgos y controles de seguridad.

4) Una vez que la unidad administrativa a cargo del tratamiento de datos personales tenga identificadas las posibles vulnerabilidades y amenazas, así como definidos los controles de seguridad preliminares –a partir del análisis realizado a los inventarios y los cuestionarios de hábitos de seguridad del personal y cumplimiento de obligaciones-, preparará una entrevista con las distintas áreas responsables de los tratamientos, a fin de intercambiar información con relación a los posibles riesgos identificados y los controles de seguridad necesarios para mitigarlos.

En las entrevistas se deberá identificar qué controles de seguridad tiene implementados el área a cargo del tratamiento.

5) A partir de la información obtenida de las distintas entrevistas, la unidad administrativa determinará los riesgos y controles de seguridad necesarios para mitigarlos.

Los riesgos vinculados a la infraestructura y recursos impresos o electrónicos serán definidos por la Gerencia de Sistemas.

Fase Tres. Entrevistas y determinación de riesgos y controles de seguridad.

6) Una vez determinados los riesgos y los controles de seguridad necesarios para mitigarlos, se realizará el análisis de brecha, que consiste en identificar cuáles son los controles que hacen falta implementar a partir de aquéllos definidos como necesarios (**Anexo 5**).

Fase Cuatro. Ponderación de los riesgos y elaboración del Plan de Trabajo.

7) Una vez que se han identificado los riesgos potenciales y determinado los controles necesarios para mitigarlos, la unidad administrativa con apoyo de la Unidad de Transparencia y la Gerencia de Sistemas, presentarán ante el Comité de Transparencia una ponderación de los riesgos, a fin de determinar cuáles se mitigarán, eliminarán, transferirán o aceptarán, así como priorizar las medidas de seguridad a implementar, cuando se actualicen las causales del artículo 36 de la Ley General de Datos.

Esta definición se podrá consultar y poner a consideración de las unidades administrativas encargadas de los tratamientos.

8) Ya que se ha realizado la ponderación, la Unidad de Transparencia elaborará el Plan de Trabajo, en el cual se definirán las acciones a implementar, priorizando las medidas de seguridad más relevantes e inmediatas.

9) En el Plan de Trabajo se deberán identificar los responsables de las acciones, así como las fechas compromiso.

Forman parte integral de este documento de seguridad el Anexo 4 el cual contiene el análisis de riesgos de la infraestructura tecnológica, software y hardware, los cuestionarios respondidos por cada unidad administrativa y la identificación de vulnerabilidades, amenazas, controles de seguridad y brechas.

El Plan de Trabajo y la ponderación de riesgos, en materia de protección de datos personales se encuentran localizados en el presente como el **Anexo 6**.

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

El artículo 33, fracción VII de la Ley General de Datos establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, el monitoreo y revisión de manera periódica de las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales.

Como se señaló, de acuerdo con la fracción VI del artículo 35 de la Ley General de Datos, los mecanismos de monitoreo y revisión forman parte del documento de seguridad.

Así, respecto a los mecanismos de monitoreo y revisión de las medidas de seguridad, el artículo 63 de los Lineamientos Generales señala lo siguiente:

> ***Monitoreo y supervisión periódica de las medidas de seguridad implementadas***
> ***Artículo 63.*** *Con relación al artículo 33, fracción VII de la Ley General, el responsable deberá evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, a fin de verificar el cumplimiento de los objetivos propuestos y, en su caso, implementar mejoras de manera continua.*
>
> *Para cumplir con lo dispuesto en el párrafo anterior del presente artículo, el responsable deberá monitorear continuamente lo siguiente:*
>
> ***I.*** *Los nuevos activos que se incluyan en la gestión de riesgos;*
> ***II.*** *Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras;*

> ***III.*** *Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;*
> ***IV.*** *La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;*
> ***V.*** *Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;*
> ***VI.*** *El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y*
> ***VII.*** *Los incidentes y vulneraciones de seguridad ocurridas.*
>
> *Aunado a lo previsto en las fracciones anteriores del presente artículo, el responsable deberá contar con un programa de auditoría, interno y/o externo, para monitorear y revisar la eficacia y eficiencia del sistema de gestión.*

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

A continuación, se desarrollan las acciones de monitoreo y supervisión periódica para las medidas de seguridad del ININ:

Mecanismos de Monitoreo

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

1) **Revisión de cumplimiento de las políticas internas del ININ por parte de las unidades administrativas, relacionadas con el tratamiento de datos personales.** Tiene el objetivo de asegurar que las personas servidoras públicas realicen los tratamientos de datos personales en concordancia con lo dispuesto en la Ley General de Datos, los Lineamientos Generales, y demás normatividad que resulte aplicable.

   Para ello, cuando se identifica algún cambio en los instrumentos antes mencionados, se deberán realizar las siguientes actividades:

   a. Revisar y, en su caso, actualizar los procesos involucrados en el tratamiento de datos personales.

   b. Revisar y, en su caso, actualizar los avisos de privacidad, las funciones y obligaciones del personal y los inventarios de datos personales, según corresponda.

c. Evaluar si hubo cambios en las amenazas, vulnerabilidades o impacto de los riesgos relacionados con las modificaciones a la normativa, para actualizar los análisis de riesgos, análisis de brecha y plan de trabajo.

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

2) **Revisión del riesgo.** Tiene el objetivo de identificar modificaciones a los riesgos identificados en los tratamientos de datos personales, para ello, se implementarán los siguientes monitoreos de las unidades administrativas que están a cargo del tratamiento de datos personales:

a. **Monitoreo del entorno físico.** Para la detección continua de amenazas y vulnerabilidades en el entorno físico, se cuenta con: (i) personal de vigilancia en los accesos al edificio del ININ, (ii) control de acceso del personal con tarjeta de proximidad, (iii) control de acceso a través de bitácoras para visitantes y personal del ININ que olvidó su credencial, (iv) control de asistencia a través de huella digital, y (v) circuito cerrado de cámaras de vigilancia.

b. **Monitoreo del entorno electrónico.** Para la detección continua de amenazas y vulnerabilidades, la GS cuenta con herramientas automatizadas de monitoreo (activo y pasivo), así como con bitácoras de los sistemas informáticos del ININ.

c. **Actualización del plan de trabajo.** Derivado del monitoreo del entorno físico o electrónico, se pueden realizar actualizaciones en el plan de trabajo en caso de que se identifiquen cambios en las amenazas, las vulnerabilidades o el impacto de los riesgos identificados. Estos cambios se pondrán a consideración del área que apoya en el análisis de riesgos, la GS y el Comité de Transparencia.

d. **Revisión de avances del plan de trabajo.** A través de los mecanismos que determine la unidad administrativa a cargo del tratamiento de datos personales, se realizará una revisión de los avances en el plan de trabajo que remitirán a la Unidad de Transparencia, identificando las acciones, fechas compromiso y, en su caso, las causas por las cuales no se está cumpliendo el plan de trabajo, para hacer los ajustes correspondientes al mismo.

e. **Actualización tecnológica.** Cuando se integren nuevos equipos de cómputo, servidores, aplicaciones o tenga lugar una migración tecnológica, se realizará una actualización del análisis de riesgo, análisis de brecha y plan de trabajo.

f. **Vulneraciones a la seguridad de los datos personales.** En caso de identificar un incidente de seguridad que involucre datos personales, la unidad administrativa a cargo del tratamiento de datos personales, la UT, la GS y el CT, se coordinarán para decidir sobre las acciones pertinentes para mitigar dicho incidente.

A continuación, se describen los mecanismos de monitoreo y revisión de este Instituto:

Elemento a revisar	Fundamento	Acciones
Los nuevos activos que se incluyan en la gestión de riesgos;	63, fracción I, de los Lineamientos Generales.	1. Revisión de cumplimiento de la normatividad, relacionada con el tratamiento de datos personales.
Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras;	63, fracción II, de los Lineamientos Generales.	1. Revisión de cumplimiento de la normatividad, relacionada con el tratamiento de datos personales.
Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;	63, fracción III, de los Lineamientos Generales.	1. Revisión de cumplimiento de la normatividad, relacionada con el tratamiento de datos personales. 2.a. Monitoreo del entorno físico. 2.b. Monitoreo del entorno electrónico.
La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;	63, fracción IV, de los Lineamientos Generales.	1. Revisión de cumplimiento de la normatividad, relacionada con el tratamiento de datos personales. 2.a. Monitoreo del entorno físico. 2.b. Monitoreo del entorno electrónico.
Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;	63, fracción V, de los Lineamientos Generales.	1. Revisión de cumplimiento de la normatividad, relacionada con el tratamiento de datos personales. 2.a. Monitoreo del entorno físico. 2.b. Monitoreo del entorno electrónico.
El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo	63, fracción VI, de los Lineamientos Generales.	1. Revisión de cumplimiento de la normatividad, relacionada con el tratamiento de datos personales. 2.c. Actualización del plan de trabajo. 2.d. Revisión de avances del plan de trabajo.
Los incidentes y vulneraciones de seguridad ocurridas.	63, fracción VII, de los Lineamientos Generales.	1. Revisión de cumplimiento de la normatividad, relacionada con el tratamiento de datos personales. 2.f. Vulneraciones a la seguridad de los datos personales.

Mecanismos de supervisión o revisión

Además del monitoreo continuo de las medidas de seguridad, se requiere realizar una supervisión periódica de las medidas de seguridad, a través de auditorías, las cuales pueden ser internas (desarrolladas por el propio ININ) o externas (realizando una contratación o a través de un convenio con un tercero).

Hasta el momento no se han realizado auditorías específicas en materia de protección de datos personales a los tratamientos del Instituto.

De conformidad con lo establecido en el artículo 151 de la Ley General de Datos y 218 de los Lineamientos Generales, este Sujeto Obligado Responsable, podrá solicitar voluntariamente al INAI la realización de una auditoría, con el objetivo de verificar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados para el cumplimiento de las disposiciones previstas en esta Ley y demás normativa que resulte aplicable.

Los resultados de las auditorías se considerarán para realizar adecuaciones al análisis de riesgos del ININ y, por lo tanto, al plan de trabajo.

VII. El programa general de capacitación.

Con relación al programa de capacitación, la fracción VIII del artículo 33 de la Ley General de Datos señala que, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá 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.

Como se señaló, de acuerdo con la fracción VII del artículo 35 de la Ley General de Datos, el programa de capacitación forma parte del documento de seguridad.

Por su parte, el artículo 64 de los Lineamientos Generales señala lo siguiente:

> ***Capacitación***
> ***Artículo 64.*** *Para el cumplimiento de lo previsto en el artículo 33, fracción VIII de la Ley General, el responsable deberá diseñar e implementar programas a corto, mediano y largo plazo que tengan por objeto capacitar a los involucrados internos y externos en su organización, considerando sus roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales y el perfil de sus puestos.*

En el diseño e implementación de los programas de capacitación a que se refiere el párrafo anterior del presente artículo, el responsable deberá tomar en cuenta lo siguiente:

I. *Los requerimientos y actualizaciones del sistema de gestión;*
II. *La legislación vigente en materia de protección de datos personales y las mejores prácticas relacionadas con el tratamiento de éstos;*
III. *Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales, y*
IV. *Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad.*

A partir de lo anterior, el ININ desarrolló su programa general de capacitación, mismo que integra el **Anexo 7** de este documento de seguridad y cuenta con la aprobación del Comité de Transparencia.

Actualización del documento de seguridad.

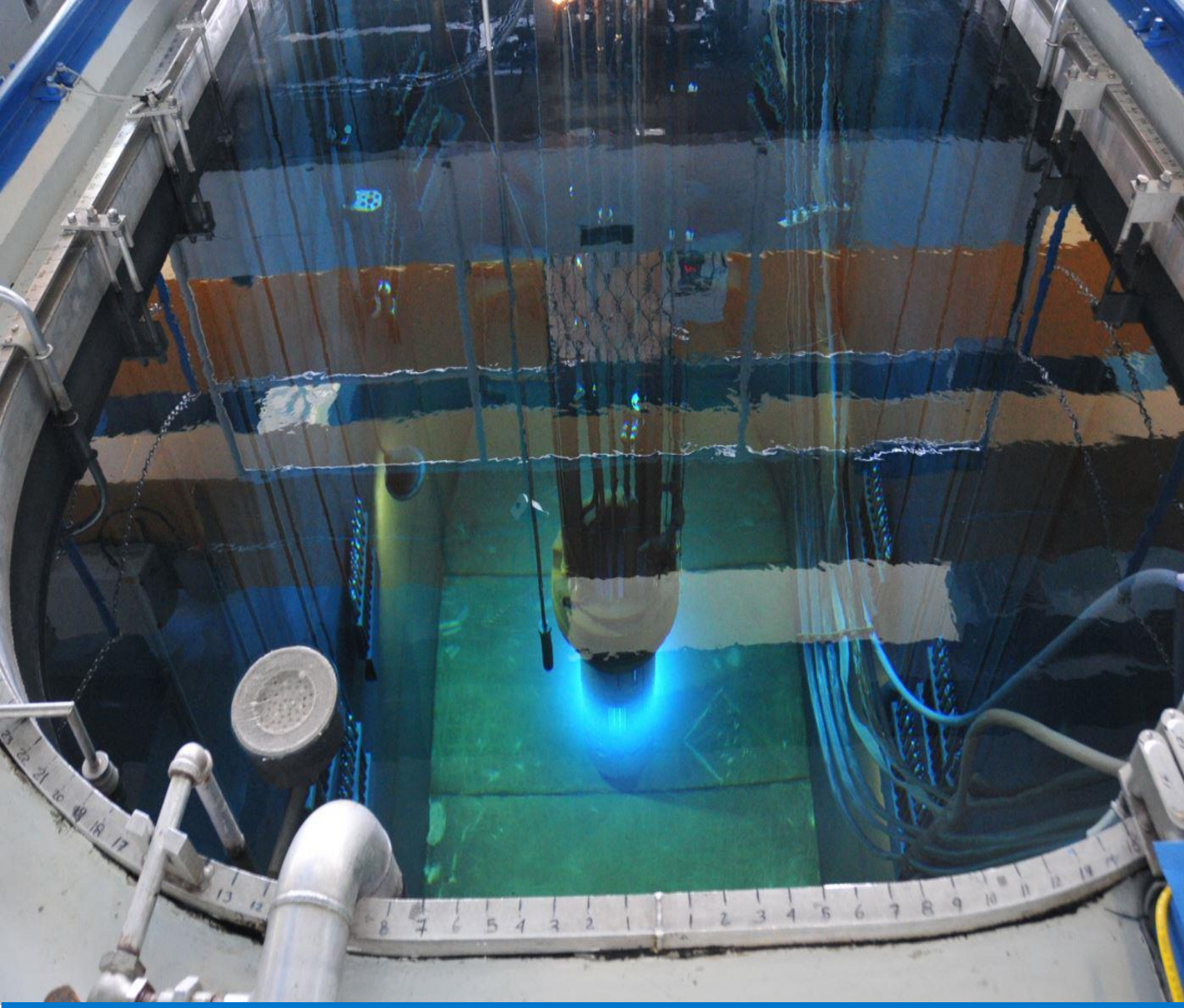
El artículo 36 de la Ley General de Datos establece la obligación de la actualización del documento de seguridad cuando ocurran los siguientes eventos:

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

En ese sentido, el Comité de Transparencia deberá estar atento a la actualización de alguno de los supuestos antes citados, para, en su caso, actualizar el presente documento de seguridad.

El siguiente cuadro muestra las fechas en que se ha actualizado el documento de seguridad del ININ:

Fecha de actualización	Motivo de la actualización
07/12/2018	Aprobación del Documento de Seguridad del ININ.



ININ