SALUD
SECRETARÍA DE SALUD

INSTITUTO NACIONAL DE CANCEROLOGÍA

Documento de Seguridad

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), cuyo objetivo es 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.

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.

El Instituto Nacional de Cancerología, en lo sucesivo INCan, es un organismo descentralizado de la Administración Pública Federal, con personalidad jurídica y patrimonio propios, agrupado en el Sector Salud, al ser sujeto obligado conforme a la Ley General, debe observar lo dispuesto por dicho instrumento normativo en el tratamiento de datos personales que lleve a cabo.

De acuerdo con lo dispuesto por los artículos 29 y 30, fracciones I y VII de la Ley General, el responsable deberá implementar mecanismos para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en dicha Ley.

La Ley General de Datos dispone que el tratamiento de datos personales que realicen los sujetos obligados estará regido por ocho principios y dos deberes, los **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, 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.

El 26 de enero de 2018, se publicaron en el Diario Oficial de la Federación los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales) cuyo objetivo es desarrollar las disposiciones previstas en la Ley General de Datos y, con ello, hacer más comprensible el cumplimiento de los principios, deberes y obligaciones exigidos en materia de protección de datos personales.

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.

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 de acuerdo a la fracción XIV del artículo 3 de la Ley General, 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.

Por lo anterior, para el debido cumplimiento de las obligaciones antes descritas, se presenta el documento de seguridad del INCan con los elementos informativos que establece el artículo 35 de la Ley General de Datos Personales.

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.

De acuerdo con la fracción I del artículo 35 de la Ley General, este inventario forma parte del documento de seguridad.

Los artículos 58 y 59 de los 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.

De lo anterior, el INCan estableció los inventarios de los distintos tratamientos de datos personales que realiza, identificando los elementos informativos que señala el artículo 58 de los Lineamientos Generales, 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**.

El siguiente cuadro muestra un resumen de los inventarios elaborados:

Área	Adscripción	Denominación del Inventario de Tratamiento de Datos Personales
Departamento de Empleo	Subdirección de Administración y Desarrollo de Personal	Sistema de nomina
Departamento de Capacitación y Desarrollo	Subdirección de Administración y Desarrollo de Personal	Reclutamiento y selección de personal
Departamento de Archivo Clínico y Bioestadística	Subdirección de Atención Hospitalaria y Consulta Externa	Expediente clínico
Departamento de Control y Referencia de Pacientes	Subdirección de Atención Hospitalaria y Consulta Externa	Registro de pacientes para preconsulta
Departamento de Trabajo Social	Subdirección de Atención Hospitalaria y Consulta Externa	Asignación Nivel socioeconómico
Subdirección de Asuntos Jurídicos	Dirección General	Notificaciones
Subdirección de Educación Médica	Dirección de Docencia	Ingreso de residencias médicas
Subdirección de Educación Médica	Dirección de Docencia	Registro de Diplomados
Subdirección de Educación Médica	Dirección de Docencia	Registro de pasantes de Servicio Social
Departamento de Tecnologías de la Información	Subdirección de Servicios Generales	Sistema INCan
Subdirección de Recursos Materiales	Dirección de Administración y Finanzas	Contrataciones

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.

De conformidad con la fracción II del artículo 35 de la Ley General, este elemento informativo forma parte del documento de seguridad.

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 INCan que trata datos personales se han identificado en dos niveles:

I. A **nivel macro**, a través del **Programa de Protección de Datos Personales** de este Instituto, en el cual se describen todas las obligaciones que establece la Ley General y los Lineamientos Generales y éstas se asociación con el área responsable de su cumplimiento, y
II. A **nivel de servidor público,** 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.

A continuación, se muestra un ejemplo de cómo se identifican las funciones y obligaciones a nivel marco en el Programa de Protección de Datos Personales, por cada una de las obligaciones que establece la Ley General y los Lineamientos Generales:

Obligaciones	*Actividades para su cumplimiento*	*Unidades administrativas y sustantivas responsables del cumplimiento*	*Medios que facilitan la acreditación del cumplimiento*
• *Sujetar el tratamiento de los datos personales a las atribuciones o facultades que la normatividad aplicable confiera al sujeto obligado, así como con estricto apego y cumplimiento de lo dispuesto en dicho ordenamiento, los Lineamientos Generales, la legislación mexicana que le resulte aplicable y, en su caso, el derecho internacional, respetando los derechos y libertades de los titulares.*	*1. Identificar el marco normativo (leyes, tratados o acuerdos internacionales, reglamentos, lineamientos, entre otros, con sus respectivos artículos) que faculta a la unidad administrativa a tratar los datos personales para cada una de las finalidades, y aquél que regula el tratamiento respectivo.*	*Todas las unidades administrativas que realicen tratamiento de datos personales.*	*Marco normativo respectivo.*

El Programa de Protección de Datos Personales forma parte integral de este documento de seguridad **Anexo 2.**

Por su parte, 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:

Servidores públicos que tienen acceso a la base de datos	*Área de adscripción*	*Finalidad del acceso*
Señalar los puestos de los servidores públicos que tienen acceso a la base de datos del tratamiento correspondiente. Uno por fila.	*Definir unidad administrativa a la que está adscrito el puesto*	*Señalar con qué fines tienen acceso los servidores públicos antes identificados. Uno por fila, según corresponda.*

El Comité de Transparencia a través de la Unidad de Transparencia, serán los responsables de dar a conocer a las personas servidoras públicas del INCan el Programa de Protección de Datos Personales, que se basa en un sistema de gestión, a fin de que el personal conozca sus funciones para el cumplimiento del sistema de gestión y las consecuencias de su incumplimiento.

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 INCan, por lo cual, para efectos del presente documento de seguridad, el marco normativo de referencia se encuentra establecido en el Manual de Organización Especifico del Instituto Nacional de Cancerología.

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;*
>
> *[...]*

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.

Asimismo, 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.*

Baja lo anteriormente 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 INCan;
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.

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
Amenazas y vulnerabilidades existentes.	33, fracción IV, de la Ley General.
Los recursos involucrados.	33, fracción IV, de la Ley General.
Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico.	60, fracción I, de los Lineamientos Generales.
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.
El valor y exposición de los activos involucrados en el tratamiento de los datos personales	60, fracción III, de los Lineamientos Generales.
Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida.	60, fracción IV, de los Lineamientos Generales.
El riesgo inherente a los datos personales tratados.	32, fracción I, de la Ley General.
La sensibilidad de los datos personales tratados.	32, fracción II, de la Ley General.
El desarrollo tecnológico.	32, fracción III, de la Ley General.
Las posibles consecuencias de una vulneración para los titulares.	32, fracción IV, de la Ley General.
Las transferencias de datos personales que se realicen.	32, fracción V, de la Ley General.
El número de titulares.	32, fracción VI, de la Ley General.
Las vulneraciones previas ocurridas en los sistemas de tratamiento.	32, fracción VII, de la Ley General.
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.

Para el proceso del análisis de riesgos se considerarán diferentes documentos de apoyo que se encuentran en el INAI como lo son la metodología de Análisis de Riego, Recomendaciones para reconocer las principales amenazas a los datos personales a partir de la valoración respecto al riesgo y Recomendaciones para el manejo de incidentes de seguridad de datos personales documentos de apoyo y que se encuentra en el **anexo 5.**

Para llevar a cabo la identificación de los riesgos relacionados con el tratamiento de datos personales, y de ello la identificación de controles de seguridad presentes o bien los que no se tengan, se realizaran las siguientes acciones:

1. Identificación del riesgo, existente o futuro, que involucre tanto físico o tecnológico.

2. Establecimiento de controles, o bien valoración de los existentes.

3. Definición de controles óptimos a través del análisis de brecha.

4. Se realizará la valoración a fin de establecer las medidas de seguridad, presentes o a implementar con apoyo de la Unidad de Transparencia y del Comité de Transparencia, conforme al plan de trabajo.

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

El artículo 33, fracción VII de la Ley General 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.

De acuerdo con la fracción VI del artículo 35 de la Ley General, los mecanismos de monitoreo y revisión forman parte del documento de seguridad. (anexo 3)

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 mejora 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 INCan:

Mecanismos de Monitoreo

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

1) **Revisión de cumplimiento de las políticas internas del INCan 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 por parte de los involucrados:

   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:

   a. **Monitoreo del entorno físico.** Para la detección continua de amenazas y vulnerabilidades en el entorno físico, se cuenta con: personal de vigilancia en los accesos a los edificios del INCan, control de acceso del personal con credencial, control de acceso a través de bitácoras para visitantes y personal del INCan que olvidó su credencial, control de asistencia a través de huella digital.
   b. **Monitoreo del entorno electrónico.** Para la detección continua de amenazas y vulnerabilidades, el Departamento de Tecnología de la Información deberá contar con herramientas automatizadas de monitoreo, así como con bitácoras de los sistemas informáticos del INCan.
   c. **Actualización del plan de trabajo.** Derivado del monitoreo del entorno físico o electrónico, se pueden realizar actualizaciones en el plan de trabajo en caso de que se identifiquen cambios en

las amenazas, las vulnerabilidades o el impacto de los riesgos identificados. Estos cambios se pondrán a consideración del área que apoya en el análisis de riesgos, el Departamento de Tecnologías de la Información y el Comité de Transparencia.

d. **Revisión de avances del plan de trabajo.** A través de los mecanismos que determine el área que apoyará en el análisis de riesgos, el Departamento de Tecnologías de la Información, la Unidad de Transparencia y el Comité de Transparencia, se hará una revisión de los avances en el plan de trabajo, identificando las acciones, fechas compromiso y, en su caso, las causas por las cuales no se está cumpliendo el plan de trabajo, para hacer los ajustes correspondientes al mismo.

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

f. **Vulneraciones a la seguridad de los datos personales.** En caso de identificar un incidente de seguridad que involucre datos personales, el área que apoya en el análisis de riesgos (UT), el Departamento de Tecnología de la Información y el Comité de Transparencia 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 las políticas internas, relacionadas 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 las políticas internas, relacionadas 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 las políticas internas, relacionadas 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 las políticas internas, relacionadas 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 las políticas internas, relacionadas 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	63, fracción VI, de los Lineamientos Generales.	1. Revisión de cumplimiento de las políticas internas, relacionadas con el tratamiento de datos personales. 2.c. Actualización del plan de trabajo. 2.d. Revisión de avances del plan de trabajo.

en un nivel inaceptable de riesgo		
Los incidentes y vulneraciones de seguridad ocurridas.	63, fracción VII, de los Lineamientos Generales.	1. Revisión de cumplimiento de las políticas internas, relacionadas 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 Instituto) o externas (realizando una contratación o a través de un convenio con un tercero).

El programa de auditoría será aquél que determine el Comité de Transparencia en el Programa de Protección de Datos Personales del INCan.

Los resultados de las auditorías se considerarán para realizar adecuaciones al análisis de riesgos del INCan, así como al plan de trabajo.

VII. El programa general 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.

De acuerdo con la fracción VII del artículo 35 de la Ley General, el programa de capacitación forma parte del documento de seguridad y definirá el artículo 64 de los Lineamientos Generales que 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.*

El programa de capacitación, se encuentra en **Anexo 4** de este documento de seguridad.

Actualización del documento de seguridad.

El artículo 36 de la Ley General 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 con apoyo de la Unidad de Transparencia, deberá generar una supervisión para la actualización de alguno de los supuestos antes citado, para que, y llegado el caso, actualizar el presente documento de seguridad.