SENER
SECRETARÍA DE ENERGÍA

CNSNS
COMISIÓN NACIONAL DE SEGURIDAD NUCLEAR Y SALVAGUARDIAS

DOCUMENTO DE SEGURIDAD

COMISIÓN NACIONAL DE SEGURIDAD NUCLEAR Y SALVAGUARDIAS

AGOSTO, 2022

Insurgentes Sur 890, Del Valle, C.P. 03100. Benito Juárez, CDMX
t: (55) 5000.6000 www.gob.mx/sener

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), la cual tiene como objetivo establecer las bases, principios y procedimientos para garantizar el derecho humano 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 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, la Comisión Nacional de Seguridad Nuclear y Salvaguardias (CNSNS) es sujeto obligado de la Ley General y, por ello, debe observar lo dispuesto por dicho instrumento normativo en el tratamiento de datos personales que lleve a cabo.

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

Dichos principios son: licitud, lealtad, información, consentimiento, finalidad, proporcionalidad, calidad y responsabilidad; mientras que los deberes son el de confidencialidad y seguridad.

Asimismo, la Ley General detalla el alcance y los procedimientos para el ejercicio de los 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 actualmente también el de portabilidad.

Estos principios, deberes y derechos imponen una serie de obligaciones para los sujetos regulados por la Ley General, que tienen como finalidad que el tratamiento se realice de manera tal que se garantice la protección de los datos personales, con el objeto de respetar el derecho a la autodeterminación informativa de los titulares.

En específico, en relación con el deber de seguridad, el artículo 31 de la Ley General 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 un posible 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 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 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 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"*.

El documento deberá contener, al menos, la siguiente información que establece el artículo 35 de la Ley General:

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, 84 del Título Séptimo de la Ley General 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 normativa aplicable como se enuncia 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 otra parte, el artículo 85 de la Ley General 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, esta Ley y demás normativa aplicable, que tendrá las siguientes funciones para efectos del tratamiento de los datos personales:

"*VII. Asesorar a las áreas adscritas al responsable en materia de protección de datos personales."*

En ese sentido, se presenta el documento de seguridad de la Comisión Nacional de Seguridad Nuclear y Salvaguardias con los elementos informativos.

Normatividad

- Constitución Política de los Estados Unidos Mexicanos DOF 05-02-1917
  Última reforma DOF 28/05/2021

  https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados DOF 26/01/2017

  https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

- Lineamientos Generales de Protección de Datos Personales para el Sector Público DOF: 26/01/2018

  http://inicio.inai.org.mx/AcuerdosDelPleno/ACT-PUB-19-12-2017.10.pdf

- Recomendaciones para el Manejo de Incidentes de Seguridad de Datos Personales. Publicación junio 2018

  https://home.inai.org.mx/wp-content/uploads/Recomendaciones_Manejo_IS_DP.pdf

- Manual de Políticas de Seguridad de la Información de la Comisión Nacional de Seguridad Nuclear y Salvaguardias.

Glosario

Análisis de brecha: Concentración de elementos específicos que pueden existir entre lo deseable y lo actual.

Análisis de riesgo: Identificar peligros y estimar los riesgos, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento.

Archivo: Conjunto organizado de documentos producidos o recibidos por los sujetos obligados en el ejercicio de sus atribuciones y funciones, con independencia del soporte, espacio o lugar que se resguarden.

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

Comité de Transparencia: El Comité de Transparencia de la Comisión Nacional de Seguridad Nuclear y Salvaguardias.

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

Datos personales sensibles: 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 preferencia sexual.

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

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

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

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 Administrativa: Las previstas en el Manual de Organización de la Comisión Nacional de Seguridad Nuclear y Salvaguardias

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

Vulneración de seguridad: En cualquier fase del tratamiento de datos, al menos, las siguientes: I. La pérdida o destrucción no autorizada; II. El robo, extravío o copia no autorizada; III. El uso, acceso o tratamiento no autorizado, o IV. El daño, la alteración o modificación no autorizada.

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

El artículo 33, fracción I 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, la elaboración de un inventario de datos personales y de los sistemas de tratamiento.

Sobre el particular, los artículos 58 y 59 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público (en lo sucesivo, 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."

A partir de lo anterior, las unidades administrativas elaboraron con acompañamiento de la Unidad de Transparencia 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.

Asimismo, a continuación, se muestra el listado de los tratamientos con inventarios elaborados:

No. CONSE.	UNIDAD ADMINISTRATIVA	ÁREA	NOMBRE DEL TRATAMIENTO (PROCESO)
1	**DIRECCIÓN GENERAL**	Dirección de Asuntos Jurídicos e Internacionales	
2			
3			

No. CONSE.	UNIDAD ADMINISTRATIVA	ÁREA	NOMBRE DEL TRATAMIENTO (PROCESO)
1	DIRECCIÓN COORDINADORA DE TECNOLOGÍA, REGLAMENTACIÓN Y SERVICIOS	Dirección de Telemática y Sistemas de Información	
2			
3			
4		Dirección de Tecnología	
5			
6			
7		Dirección de Reglamentación y Capacitación Técnica Básica	
8			
9			

No. CONSE.	UNIDAD ADMINISTRATIVA	ÁREA	NOMBRE DEL TRATAMIENTO (PROCESO)
1		Dirección de Evaluación	
2			

3	**DIRECCIÓN COORDINADORA DE SEGURIDAD NUCLEAR**		
4		Dirección de Verificación Operativa	
5			
6			
7		Dirección de Acciones Reguladoras	
8			
9			

No. CONSE.	UNIDAD ADMINISTRATIVA	ÁREA	NOMBRE DEL TRATAMIENTO (PROCESO)
1		Dirección de Aplicaciones Médicas	
2			
3			

4	**DIRECCIÓN COORDINADORA DE SEGURIDAD RADIOLÓGICA**	Dirección de Programas Institucionales y Documentación	
5			
6		Dirección de Aplicaciones Industriales	
7		Dirección de Emergencias y Eventos de Alto Impacto	
8			
9			

No. CONSE.	UNIDAD ADMINISTRATIVA	ÁREA	NOMBRE DEL TRATAMIENTO (PROCESO)
1		Dirección de Seguridad física y Salvaguardias	
2			
3			

4	**DIRECCIÓN COORDINADORA DE VIGILANCIA RADIOLÓGICA AMBIENTAL, SEGURIDAD FÍSICA Y SALVAGUARDIAS**	Dirección de Vigilancia Radiológica Ambiental	
5			
6			
7		Dirección de Gestión de Desechos e Impacto Radiológico Ambiental	
8			
9			

No. CONSE.	UNIDAD ADMINISTRATIVA	ÁREA	NOMBRE DEL TRATAMIENTO (PROCESO)
1		Subdirección de Recursos Humanos	
2			
3			
4			
5			

	DIRECCIÓN DE FINANZAS Y ADMINISTRACIÓN	Subdirección de Recursos Materiales	
6			
7		Subdirección de Presupuestos	
8			
9			
10		Subdirección de Contabilidad	
11			
12			
13		Subdirección de Integración, Seguimiento y Control	
14			
15			
16		Subdirección de Servicios Generales	
17			
18			

19		Unidad de Transparencia	
20			
21			

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

El artículo 33, fracción II 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, 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, 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 de la CNSNS 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 las siguientes columnas:

DIRECCIÓN GENERAL

Servidores públicos que tienen acceso a la base de datos (15)	***Área de adscripción (16)***	***Finalidad del -+ acceso (17)***
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.*

DIRECCIÓN COORDINADORA DE TECNOLOGÍA, REGLAMENTACIÓN Y SERVICIOS

Servidores públicos que tienen acceso a la base de datos (15)	***Área de adscripción (16)***	***Finalidad del -+ acceso (17)***
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.*

DIRECCIÓN COORDINADORA DE SEGURIDAD NUCLEAR

Servidores públicos que tienen acceso a la base de datos (15)	***Área de adscripción (16)***	***Finalidad del -+ acceso (17)***
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.*

DIRECCIÓN COORDINADORA DE SEGURIDAD RADIOLÓGICA

Servidores públicos que tienen acceso a la base de datos (15)	***Área de adscripción (16)***	***Finalidad del -+ acceso (17)***
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.*

DIRECCIÓN COORDINADORA DE VIGILANCIA RADIOLÓGICA AMBIENTAL, SEGURIDAD FÍSICA Y SALVAGUARDIAS

Servidores públicos que tienen acceso a la base de datos (15)	***Área de adscripción (16)***	***Finalidad del -+ acceso (17)***
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.*

DIRECCIÓN DE FINANZAS Y ADMINISTRACIÓN

Servidores públicos que tienen acceso a la base de datos (15)	***Área de adscripción (16)***	***Finalidad del -+ acceso (17)***
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.*

Adicionalmente, conviene señalar que las funciones y obligaciones del personal que trata datos personales se encuentran definidas en la legislación y normatividad interna que rige el actuar de la CNSNS, por lo cual, para efectos del presente documento de seguridad, se encuentra establecido en el Reglamento Interior de la Secretaría de Energía, así como en el Manual de Organización de la CNSNS. (Anexo 2).

Asimismo, la Dirección de Telemática y Sistemas de la Información, adscrita a la Dirección Coordinadora de Tecnología, Reglamentación y Servicios emitió las Políticas de Seguridad de Comisión Nacional de Seguridad Nuclear y Salvaguardias (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 la CNSNS 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; todo lo anterior en apego a las fracciones I y X del Artículo 30 del Reglamento Interior de la Secretaría de Energía. publicado el 31 de octubre de 2014 en el Diario Oficial de la Federación.

Estas Políticas de Seguridad de información de la Comisión Nacional de Seguridad Nuclear y Salvaguardias se deben aplicar independientemente de la manera en que se presenta la información (impresa, manuscrita, 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 de la CNSNS. 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 en la Institución.

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 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, 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, 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.

Por lo dispuesto en los artículos citados, dicho 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 de la CNSNS;
3. Análisis de riesgos de vulneraciones, 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 la CNSNS, 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.

Además, 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, como sigue:

a) Datos personales con riesgo inherente bajo: Considera datos de identificación y contacto o información académica o laboral, tal como nombre, teléfono, 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 encuentren en 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 incluye 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 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 del riesgo inherente del dato personal, así como el nivel se 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 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.	• Análisis de riesgos de la infraestructura tecnológica y recursos de software y hardware; • Análisis de riesgos de hábitos de seguridad del personal de la CNSNS; • Análisis de riesgos de vulneraciones, y • Análisis de riesgos vinculado con el cumplimiento de obligaciones normativas en materia de datos personales.	En los cuatro cuestionarios o fuentes se identifican las vulnerabilidades y amenazas específicas.
Tomar en cuenta los recursos involucrados.	33, fracción IV, de la Ley General.	• Análisis de riesgos de la infraestructura tecnológica y recursos de software y hardware, y • Análisis de riesgos de vulneraciones.	La primera fuente refiere específicamente a los recursos de hardware y software; mientras que 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.

Elemento requerido	Fundamento	Fuente	Observaciones
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 con 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 de la CNSNS.	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.
El riesgo inherente a los datos personales tratados.	32, fracción I, de la Ley General.	• Análisis de riesgos de vulneraciones.	En el inventario se identifica el tipo de datos tratado y las finalidades del

Elemento requerido	Fundamento	Fuente	Observaciones
			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.	• 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.	• Análisis de riesgos de la infraestructura tecnológica y recursos de software y hardware.	En el análisis realizado por la DCTRS 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.	• 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.	• Análisis de riesgos de vulneraciones.	En el inventario se identifican las transferencias, lo que es considerado al momento de determinar riesgos y

Elemento requerido	Fundamento	Fuente	Observaciones
			controles de seguridad.
El número de titulares.	32, fracción VI, de la Ley General.	• 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.	• 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.	• 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 tener los datos personales tratados para una tercera persona no autorizada para su posesión, para la priorización y determinación del tratamiento del riesgo.

Existen grandes retos a los que se enfrentan todas las instituciones, tanto públicas como privadas, uno de ellos es el 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 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; en el documento denominado Recomendaciones para el Manejo de Incidentes de Seguridad de Datos Personales, emitidas por el INAI, se indican los incidentes 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, y
5. Acceso ilegal a las bases de datos personales por un externo

El proceso del 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 5).

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

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

2. La unidad administrativa a cargo de tratamientos 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 Dirección Coordinadora de Tecnologías, Reglamentación y Servicios (DCTRS) 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 de 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 deberán 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 los controles de seguridad necesarios para mitigarlos.

   Los riesgos vinculados a la infraestructura y recursos impresos o electrónicos serán definidos por la DCTRS.

Fase Tres. Análisis de brecha

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 4).

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 DCTRS 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.

En la ponderación se deberán tomar en cuenta las posibles consecuencias de una vulneración para los titulares, el número de titulares y el riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados por una tercera persona no autorizada para su posesión.

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 fecha compromiso.

Forman parte integral de este documento de seguridad el Anexo 5 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 encuentra localizado 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 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, 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.*

…”

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 la CNSNS.

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

Mecanismos de Monitoreo de las unidades administrativas que están a cargo del tratamiento de datos personales

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

1) **Revisión de cumplimiento de las políticas de la CNSNS por parte de las unidades administrativas, relacionadas con el tratamiento de datos personales.** Su objetivo es asegurar que los servidores públicos realicen los tratamientos de datos personales en relación con lo dispuesto en la Ley

General, los Lineamientos Generales, y demás normatividad que resulte aplicable en materia de protección de datos personales.

Para ello, cuando se identifique algún cambio en los instrumentos normativos 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, (ii) control de acceso del personal con tarjeta, (iii) control de acceso a través de bitácoras para visitantes y personal que olvidó su credencial.
b. Monitoreo del entorno electrónico. Para la detección continua de amenazas y vulnerabilidades, la DCTRS cuenta con herramientas automatizadas de monitoreo (activo y pasivo), así como con bitácoras de los sistemas informáticos.
c. Actualización del plan de trabajo. Derivado del monitoreo del entorno físico o electrónico, se pueden realizar actualizaciones en el plan de trabajo en caso de que se identifiquen cambios en las amenazas, las vulnerabilidades o el impacto de los riesgos identificados. Estos cambios se pondrán a consideración del área que apoya en el análisis de riesgos, la DCTRS y el Comité de Transparencia
d. Revisión de avances del plan de trabajo. Con base en los mecanismos que determine la unidad administrativa a cargo del tratamiento de datos personales se realizará un informe 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.** La unidad administrativa a cargo del tratamiento de datos personales deberá informar sin dilación alguna, en términos del artículo 41 de la Ley General, al titular de los datos personales, a la Unidad de Transparencia, a DCTRS, al Comité de Transparencia, las vulneraciones que afecten de forma significativa los derechos patrimoniales o morales, en cuanto se confirme que ocurrió la vulneración y que haya empezado a tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, a fin de que los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos.

A continuación, se describen los mecanismos de monitoreo y revisión de la CNSNS:

Elemento a revisar	Fundamento	Acciones
Los nuevos activos que se incluyan en la gestión de riesgos;	63, fracción I, de los Lineamientos Generales.	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.	Revisión de cumplimiento de la normatividad relacionada con el tratamiento de datos personales. Actualización tecnológica.
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.	Revisión de cumplimiento de la normatividad relacionada con el tratamiento de datos personales. Monitoreo del entorno físico. Monitoreo del entorno electrónico.
La posibilidad de que vulnerabilidades nuevas o incrementadas sean	63, fracción IV, de los Lineamientos Generales.	Revisión de cumplimiento de la normatividad relacionada con el tratamiento de datos personales.

Elemento a revisar	Fundamento	Acciones
explotadas por las amenazas correspondientes;		Monitoreo del entorno físico. 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.	Revisión de cumplimiento de la normatividad relacionada con el tratamiento de datos personales. Monitoreo del entorno físico. 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.	Revisión de cumplimiento de la normatividad relacionada con el tratamiento de datos personales. Actualización del plan de trabajo. Revisión de avances del plan de trabajo.
Los incidentes y vulneraciones de seguridad ocurridas.	63, fracción VII, de los Lineamientos Generales.	Revisión de cumplimiento de la normatividad relacionada con el tratamiento de datos personales. Vulneraciones a la seguridad de los datos personales.

Mecanismos de supervisión y revisión

Además del monitoreo continuo de las medidas de seguridad, se estará a lo dispuesto en el artículo 30 fracción V de la Ley General.

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

Los resultados obtenidos de los monitoreos o revisiones internas se considerarán para realizar adecuaciones al análisis de riesgos y, en su caso, 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 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, 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, se desarrolló el programa general de capacitación, mismo que integra el Anexo 7 de este documento de seguridad y que cuenta con la aprobación del Comité de Transparencia.

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.

Las unidades administrativas informarán a la Unidad de Transparencia las modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo; aquellos resultados de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión; los resultados de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida y las acciones correctivas y preventivas ante una vulneración de seguridad, a fin de que sean sometidas ante el Comité de Transparencia para la debida actualización del presente documento.