



**GOBIERNO DE
MÉXICO**



CONAHCYT

CONSEJO NACIONAL DE HUMANIDADES
CIENCIAS Y TECNOLOGÍAS

UNIDAD DE ASUNTOS JURÍDICOS

DIRECCIÓN DE CONSULTA Y ESTUDIOS NORMATIVOS

SUBDIRECCIÓN DE TRANSPARENCIA Y SEGUIMIENTO LEGISLATIVO

DOCUMENTO DE SEGURIDAD CONAHCYT



CONTENIDO

- I. Presentación
- II. Inventario de datos personales y de los sistemas de tratamiento
- III. Obligaciones de las personas servidoras públicas que tratan datos personales en el Conahcyt
- IV. Análisis de riesgos
- V. Análisis de Brecha
- VI. Plan de Trabajo
- VII. Mecanismos de monitoreo
- VIII. Medidas de Seguridad
- IX. Programa de capacitación
- X. Actualización del Documento de Seguridad.



I. PRESENTACIÓN

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

La Constitución Política de los Estados Unidos Mexicanos, establece el derecho de los titulares de los datos personales el poder ejercer los derechos de acceso, rectificación, cancelación y oposición, y el de portabilidad.

El artículo 3 fracción XIV de la LGPDPPSO, define el documento de seguridad, 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 de seguridad es un componente esencial dentro del marco legal establecido, ya que se regula el tratamiento legítimo, controlado e informado de los datos personales por parte del Consejo Nacional de Humanidades Ciencias y Tecnologías, siendo su propósito principal, establecer las medidas técnicas y organizativas necesarias para proteger la confidencialidad, integridad y disponibilidad de los datos personales, así como prevenir su pérdida, uso indebido, acceso no autorizado o divulgación.

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.

Licitud
Lealtad
Información
Consentimiento
Finalidad
Proporcionalidad
Calidad
Responsabilidad

Asimismo, se cuenta con deberes de confidencialidad y de seguridad, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en su artículo 31 señala



que los responsables del tratamiento establecerán y mantendrán 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, asimismo la citada ley en su artículo 33 establece 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.*

De igual forma, la Ley General, señala en su artículo 35 que es obligación de los responsables de manera particular, deberán elaborar un documento de seguridad que contenga, al menos, lo siguiente:

- El inventario de datos personales y de los sistemas de tratamiento;
- Las funciones y obligaciones de las personas que traten datos personales;



- El análisis de riesgos;
- El análisis de brecha;
- El plan de trabajo;
- Los mecanismos de monitoreo y revisión de las medidas de seguridad
- El programa general de capacitación.

II. EL INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO.

El artículo 33, fracción I de la Ley General de Protección de Datos Personales, señala actividades para la implementación de medidas de seguridad para la protección de datos personales, y la elaboración de un inventario de datos personales y de los sistemas de tratamiento.

El artículo 35 fracción I, de la Ley General, establece que el inventario forma parte del documento de seguridad.

Los lineamientos Generales de Protección de Datos Personales para el Sector Público, señalan en los artículos 58 y 59 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:*

- El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales;*
- Las finalidades de cada tratamiento de datos personales;*
- El catálogo de los tipos de datos personales que se tratan, indicando si son sensibles o no;*
- El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales;*
- La lista de servidores públicos que tienen acceso a los sistemas de tratamiento;*

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.

El Consejo Nacional de Humanidades Ciencias y Tecnologías. considerará lo siguiente:

Identificación de datos personales: Se identificarán todos los tipos de datos personales que se recaban o procesan. Esto puede incluir información como nombres, direcciones, números de identificación, información de contacto, detalles financieros, registros de salud, entre otros.

Fuentes de datos: Se determinará de dónde provienen los datos personales, pueden ser recopilados directamente de los titulares, a través de formularios en línea, o bien por otros medios.

Propósito del Tratamiento: Se deberá documentar el propósito para el cual se recaban y se tratan los datos personales.

Ubicación y almacenamiento: Se registrarán los lugares dónde se almacenan los datos personales, ya sea en servidores locales, en la nube, en dispositivos y también quién tiene acceso a estos datos y con qué fines.

Categorización de datos sensibles: Se deberá Identificar y clasificar los datos personales sensibles o especiales que se tratan.

Consentimiento: Se deberá si se cuenta con el consentimiento adecuado de los titulares para tratar sus datos personales.



Gestión de riesgos: Se evaluarán los riesgos asociados con el manejo y tratamiento de los datos personales, como posibles brechas de seguridad, acceso no autorizado y pérdida de datos.

Registro de actividades de tratamiento: Se deberán registrar todas las actividades relacionadas con el tratamiento de datos personales, incluyendo quién accede a los datos y con qué propósito.

Actualización: Se deberá mantener actualizado el inventario de datos personales y se revisará periódicamente para garantizar su precisión.

Los inventarios tanto de datos personales como de sistemas de datos personales forman parte integral de este documento de seguridad y se encuentran contenidos en el **anexo 1**.

II. LAS FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATEN DATOS PERSONALES.

El artículo 33, fracción II de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, señala que 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.

Asimismo, el artículo 35 fracción II, de la Ley General, señala las funciones y obligaciones de las personas que traten datos personales y este elemento forma parte del Documento de Seguridad.

El artículo 57 de los Lineamientos Generales señala:

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.



Asimismo, el Comité de Transparencia es el órgano colegiado responsable de dar a conocer a las personas servidoras públicas del Conahcyt, respecto del Programa de Protección de Datos Personales, con la finalidad de que las personas servidoras públicas, conozcan los alcances del mismo, e identifiquen sus funciones para el cumplimiento del sistema de gestión y las consecuencias de su incumplimiento.

IV. ANÁLISIS DE RIESGOS

El artículo 33, fracción IV, 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.

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:*

- 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;*

La realización del análisis de riesgo de datos personales es fundamental para salvaguardar la privacidad de los individuos y garantizar el cumplimiento de la normatividad, su importancia radica en aspectos clave ya que se consideran evaluaciones cuantitativas y cualitativas respecto de los activos de información, determinando causas y consecuencias relativas a las amenazas y vulnerabilidades a las que están expuestos los sistemas que tratan los datos personales, permitiendo establecer los parámetros y medidas de posibles vulneraciones de seguridad.

Los Lineamientos Generales para la protección de datos Personales para el Sector Público, señalan en su artículo 60 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.

V. ANÁLISIS DE BRECHA

El artículo 33, fracción V, 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 brecha.

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:

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

La realización del análisis de brecha va enfocado a la seguridad de los datos personales recabados, es el proceso en el que se identifican y evalúan las posibles vulnerabilidades en la seguridad de la información personal, busca identificar y corregir las vulnerabilidades que podrían resultar en una filtración o robo de datos personales de clientes, empleados u otros individuos, este análisis incluye la evaluación de los controles de seguridad existentes, la identificación de posibles puntos débiles en la protección de los datos, y la implementación de medidas correctivas para reducir o eliminar las vulnerabilidades identificadas, dicho proceso es importante para garantizar la confidencialidad, integridad y disponibilidad de la información personal, por lo cual permite evaluar de forma amplia las prácticas de seguridad llevadas a cabo y así poder establecer las acciones que se deben implementar a efecto de disminuir la brecha entre la forma actual de manejo y las mejores prácticas, toda vez que se deben tomar decisiones respecto de los niveles de riesgo.

Los Lineamientos Generales para la protección de datos Personales para el Sector Público, señalan en su artículo 61 lo siguiente:



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.

VI. PLAN DE TRABAJO

De conformidad con lo establecido en el artículo 33 fracción VI, de la Ley General de Protección de Datos Personales en posesión de los Sujetos Obligados, el responsable deberá:

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;*

Este documento que especifica las actividades, recursos y tiempos necesarios para llevar a cabo las acciones a realizar y es fundamental para establecer objetivos, definir las responsabilidades de cada miembro del equipo, y establecer un cronograma detallado para cumplir con los plazos establecidos, permitiendo así tener un seguimiento de las actividades realizadas.

Los Lineamientos Generales para la protección de datos Personales para el Sector Público, señalan en su artículo 62 lo siguiente:

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.

El Plan de Trabajo forma parte integral de este documento de seguridad y se encuentra contenido en el **anexo 2**.

VII. MECANISMOS DE MONITOREO

De conformidad con el artículo 33, fracción VII de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, se establece que 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.

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

Los Lineamientos Generales para la protección de datos Personales para el Sector Público, señalan en su artículo 63 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 acuerdo con la fracción VI, del artículo 35 de la Ley General, los mecanismos de monitoreo y revisión forman parte del documento de seguridad.

VIII. MEDIDAS DE SEGURIDAD

Las medidas de seguridad físicas son las medidas, mecanismos y controles que se adoptan para proteger el entorno físico en el que los datos personales son tratados, incluyendo incluso la disposición de medios de almacenamiento.

Las medidas de seguridad técnicas se refieren a las medidas, mecanismos y controles tecnológicos para protección de los datos personales tratados en entornos digitales y los recursos que se involucran en su tratamiento.

Las medidas de seguridad administrativa, entendidas como el conjunto de medidas, mecanismos y controles que se traducen en políticas y procedimientos cuyo fin es que a nivel organizacional se protejan los datos personales sometidos a tratamiento.

Se identificará el nivel de medidas de seguridad que serán adoptadas para la salvaguardar los datos personales.

El **riesgo inherente** a los datos personales. Se deben documentar las probabilidades de que una amenaza se configure con respecto a que las medidas de seguridad sean vulneradas y



los datos personales sean expuestos o pierdan sus características de confidencialidad, disponibilidad e integridad.

La **sensibilidad** de los datos personales.

- Si se trata de 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 referencia sexual.
- 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 el titular.

Debido a lo anterior, atendiendo a la clasificación que se realice, se deberá ponderar el nivel de sensibilidad de los datos personales sometidos a tratamiento.

Desarrollo tecnológico. El criterio debe ser considerado en dos dimensiones:

- El desarrollo comercial existente.
- El desarrollo que es aplicado por sujeto obligado que realiza el tratamiento de los datos personales, el que debe estar justificados técnica y económicamente.

Las posibles **consecuencias de una vulneración** a los titulares. Este criterio está íntimamente relacionado con el riesgo inherente, pues se deben documentar las posibilidades y consecuencias de una vulneración a los datos personales de los titulares, la que se debe realizar tomando en cuenta el tipo de dato y las características de sus titulares.

Las **transferencias** de datos personales que se realicen. Se deben considerar las comunicaciones que se realizan a terceros ajenos a la organización bajo la figura de transferencia.

El **número de titulares**. Se trata de un criterio importante, pues del mismo se desprende la cantidad de datos tratados, que mientras más elevado sea en número, mayor es el atractivo para su vulneración.

Las **vulneraciones previas** que hubieren ocurrido a los datos personales.



El **riesgo por el valor potencia cuantitativo o cualitativo** que los datos personales pueden tener para volverse atractivos a ser vulnerados.

Los mecanismos de monitoreo y revisión de las medidas de seguridad, forman parte de este documento de seguridad y se encuentran contenidos en el **anexo 3**.

IX. PROGRAMA DE CAPACITACIÓN

El 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.

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.*

El Programa de capacitación, forma parte de este documento de seguridad y se encuentra contenido en el **anexo 4**.



X. 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 deberá estar atento a la actualización de alguno de los supuestos y en su caso, estar en posibilidad de actualizar el presente documento de seguridad.

Las unidades administrativas informarán a la UT 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.