



---

**FGR**

**FISCALÍA GENERAL  
DE LA REPÚBLICA**

---

# **DOCUMENTO DE SEGURIDAD**

**Fiscalía General de la República**

## CONTENIDO

### Contenido

INTRODUCCIÓN -----	3
MARCO NORMATIVO-----	4
DEBER DE SEGURIDAD-----	5
ÁMBITO DE APLICACIÓN-----	6
METODOLOGÍA -----	7
MEDIDAS DE SEGURIDAD DE LOS DATOS PERSONALES EN LA FISCALÍA GENERAL DE LA REPÚBLICA -----	8
PRACTICAS EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN -----	9
INTEGRACIÓN DEL DOCUMENTO DE SEGURIDAD DE LA FISCALÍA GENERAL -----	10
EL INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO-----	11
FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATEN DATOS PERSONALES -----	14
ANÁLISIS DE RIESGO -----	15
ANÁLISIS DE BRECHA -----	16
PLAN DE TRABAJO -----	17
LOS MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD. -----	18
PROGRAMA GENERAL DE CAPACITACIÓN -----	19
ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD -----	20

## INTRODUCCIÓN

A partir de enero de 2017 se publicó la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados en adelante Ley General, la cual tiene como objetivo establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales que estén en posesión de los sujetos obligados.

Al respecto, 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 Fiscalía General de la República (**FGR**), como órgano autónomo encargado de investigar y perseguir delitos de orden federal<sup>1</sup> con carácter de sujeto obligado, tiene el deber de proteger los datos personales en su posesión, e implementar mecanismos que acrediten el cumplimiento a los principios, deberes, derechos y demás obligaciones establecidas en Ley General, de acuerdo con sus atribuciones.

Por otra parte, de conformidad con lo dispuesto en los artículos 29 y 30, fracciones I y VII de la Ley General, se deberán implementar mecanismos para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en dicha Ley, aunado a lo anterior, dispone que el tratamiento de datos personales que realicen los sujetos obligados estará regido por ocho principios y dos deberes, teniendo como principios el de 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.

En esas consideraciones, el artículo 35 de la Ley General establece como una obligación la elaboración de un **documento de seguridad**, que de conformidad con la fracción XIV del artículo 3 de la Ley antes referida se define 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 cual, 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.

---

<sup>1</sup> Artículo 21 y 102 de la CPEUM

## MARCO NORMATIVO

Los instrumentos normativos que tutelan a la protección de datos personales en posesión de esta Fiscalía General de la República, son los siguientes:

- Artículos 6 y 16 de la Constitución Política de los Estados Unidos Mexicanos.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Ley de la Fiscalía General de la República.
- Estatuto Orgánico de la Fiscalía General de la República
- Lineamientos Generales de Protección de Datos Personales para el Sector Público, emitidos por el INAI.

## DEBER DE SEGURIDAD

De conformidad con lo establecido en el artículo 31 de la Ley General, con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable tendrá el deber de establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan:

- Protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado.
- Garantizar su confidencialidad, integridad y disponibilidad.

En esas consideraciones, el artículo 35 de la Ley General, dispone de manera particular en atención a dichas medidas la elaboración de un Documento de Seguridad.

Por lo que, en atención al deber de seguridad de los datos personales, en los sistemas de tratamiento de datos personales de la Fiscalía General de la República se debe atender lo siguiente:



## ÁMBITO DE APLICACIÓN

Respecto a los deberes que hace referencia la Ley General, este documento es aplicable para todas las unidades pertenecientes a la FGR que, en el ejercicio de sus funciones y atribuciones, lleven a cabo una administración de bases de datos en sistemas de tratamiento de datos personales, ya sea sistemas completos o el segmento de información que le sea correspondiente.

De igual forma serán aplicables al tratamiento de datos personales que obren en soportes físicos o electrónicos, con independencia de la forma o modalidad de su creación, procesamiento u almacenamiento.

Todos los servidores públicos que dentro de sus atribuciones tengan acceso a los datos personales así como al tratamiento de los mismos en cualquiera de sus fases, estarán obligados a conocer y aplicar las medidas de seguridad propias de cada sistema en el que se concentren los datos, observando en todo momento los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales, tal como lo establece el artículo 16 de la ley en mención.

## METODOLOGÍA

La integración del Documento de Seguridad de la FGR como producto de las acciones realizadas respecto a los deberes por parte de las áreas responsables, así como de la Unidad de Transparencia, llevando a cabo las siguientes acciones respectivamente;

Por parte de la Unidad de Transparencia:

- I. Establecer comunicación con las áreas responsables, con el propósito de llevar a cabo las actividades necesarias para la elaboración de su documento de seguridad correspondiente.
- II. Brindar acompañamiento a las áreas para el cumplimiento de los Deberes.
- III. Elaborar materiales de apoyo (manuales, guías, formatos, metodologías, procedimientos) para la generación del Documento de Seguridad.
- IV. Llevar a cabo cursos y capacitaciones en materia de protección de datos personales con enfoque en seguridad, durante toda la ejecución de las actividades.
- V. Dentro de cada reunión con las áreas correspondientes remite los puntos tratados, los compromisos adquiridos y los plazos para su cumplimiento.
- VI. Llevar a cabo la revisión del Documento de Seguridad con la finalidad de que cumpla con todos los parámetros establecidos en el artículo 35 de la Ley General y, en su caso, emitir observaciones pertinentes.

Por parte de las unidades administrativas responsables deberán:

- I. Establecer comunicación con la Unidad de Transparencia para dar seguimiento a las actividades de cumplimiento.
- II. Hacer de conocimiento a la Unidad de Transparencia el proceso de tratamiento de los datos personales.
- III. Cumplir con los elementos que integran el documento de seguridad establecidos en el artículo 35 de la Ley General.
- IV. Remitir el documento del sistema de gestión de datos personales generado, a la Unidad de Transparencia para su revisión y observaciones pertinentes.
- V. Presentar el documento ante el Comité de Transparencia, para fines de supervisión, mismo que será actualizado por el responsable cuando ocurran las hipótesis previstas dentro del artículo 36 de la Ley General.

## **MEDIDAS DE SEGURIDAD DE LOS DATOS PERSONALES EN LA FISCALÍA GENERAL DE LA REPÚBLICA**

Las medidas de seguridad de los datos personales se definen como el conjunto de acciones, actividades, controles o mecanismos que permiten protegerlos a los datos frente a un daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, garantizando con ello su confidencialidad, integridad y disponibilidad.

Como ya se ha referido, esas medidas pueden ser de tipo administrativo, físicas y técnicas, las cuales, de conformidad con lo establecido en el artículo 3, fracciones XXI, XXII y XXIII de la Ley General, se describen a continuación:

### **Medidas de Seguridad Administrativas**

- Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales

### **Medidas de seguridad físicas**

Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

- a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
- b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
- c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y
- d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad;

### **Medidas de seguridad técnicas**

Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

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

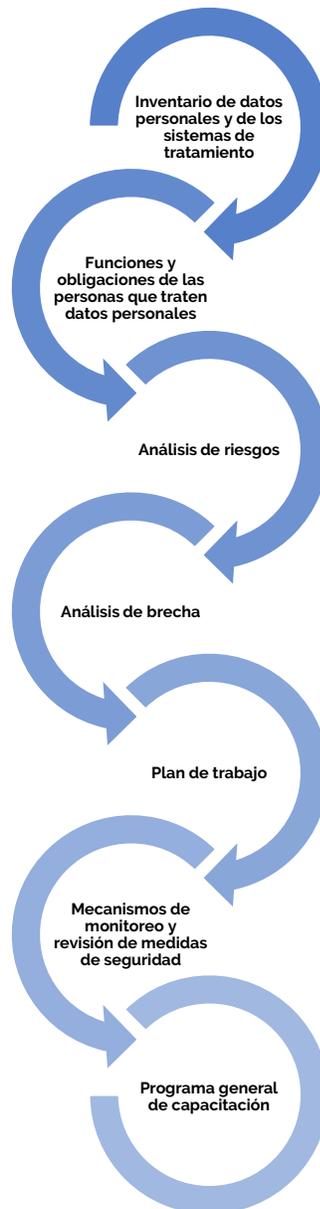
## PRACTICAS EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN

Como practicas generales, las personas servidoras públicas que lleven a cabo el tratamiento de datos personales, tienen que llevar a cabo lo siguiente:

- Tener su espacio de trabajo sin documentación importante a la vista.
- Cerrar los archiveros y resguardar la información personal bajo su custodia.
- Evitar dejar los documentos sobre impresoras.
- Realizar la eliminación segura de información en equipos de cómputo o cualquier otro medio de almacenamiento electrónico.
- Fijar plazos para la detención y eliminación de los datos personales en su posesión.
- Fomentar una cultura de la seguridad de la información.
- Bloquear o suspender las sesiones iniciadas en los equipos de cómputo
- Cerciorarse del destinatario antes de enviar información.

## INTEGRACIÓN DEL DOCUMENTO DE SEGURIDAD DE LA FISCALÍA GENERAL

Derivado de la identificación de los sistemas de tratamiento de datos personales se llevó a cabo la elaboración del presente documento de seguridad, el cual contiene los siguientes elementos:



## EL INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO

El inventario de datos es parte de las acciones encaminadas a garantizar la seguridad de los datos personales, por lo que puede entenderse como el control documentado que se llevará de los tratamientos que realizan las unidades administrativas, realizado con orden y precisión.

En esta etapa se tiene que documentar un listado de todos los sistemas de tratamiento físicos y electrónicos donde se efectúe tratamiento de datos y se realice una clasificación de todos los datos personales.

Al respecto, el inventario de datos personales y de los sistemas de tratamiento, se debe elaborar conforme a lo establecido en el artículo 33 de la Ley General, con relación al artículo 58 de los Lineamientos Generales, los cuales, disponen 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:*

*[...]*

**IV. Elaborar un inventario de datos personales y de los sistemas de tratamiento;**

*[...]"*

### **"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."*

Aunado a los elementos establecidos en el artículo 58 de los Lineamientos Generales referidos, en la elaboración del inventario se considera el ciclo de vida de los datos personales, conforme a lo dispuesto en el artículo 59 de los Lineamientos Generales, mismo que establece lo siguiente:

### **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."*

En esas consideraciones, el inventario de datos se encuentra vinculado con la información básica que permite conocer el tipo de tratamiento al se someten los datos personales, información relacionada con el ciclo de vida, tomando en consideración los siguientes elementos:

- Obtención
- Almacenamiento
- Uso, conforme a:
  - Acceso
  - Manejo
  - Aprovechamiento
  - Monitoreo
  - Procesamiento
- Divulgación:
  - Remisiones
  - Transferencias
- Bloqueo
- Cancelación, supresión o destrucción

Con la finalidad de plasmar los elementos contenidos en el inventario de datos personales, se consideraron las siguientes preguntas:

1. ¿Qué fundamento jurídico y atribuciones de la unidad administrativa identifica para realizar el tratamiento?, es necesario identificar el fundamento jurídico que habilita el tratamiento y las atribuciones de la unidad administrativa que la facultan para realizarlo.
2. ¿Qué tipo de datos personales recabo?, preguntándose si es necesario recabarlos o no, con la finalidad de utilizar sólo los necesarios para el ejercicio de sus funciones.
3. ¿Cómo recabo esos datos personales?, para identificar en qué tipo de formatos se recaban y almacenan los datos.
4. ¿Dónde se almacenan los datos personales?, almacenado en una o más ubicaciones, tanto físicas o electrónicas.
5. ¿Quién tiene permiso para acceder o manejar los datos personales?, diversas personas pueden tener acceso a los sitios donde se almacenan los datos personales. Éstas pueden tener permisos específicos.

De manera enunciativa, en los inventarios de datos, se consideraron las siguientes secciones:

## **Identificación de la unidad administrativa que declara el sistema de tratamiento de datos personales**

En esta sección se identificó puntualmente la información concerniente a la unidad administrativa que está declarando el sistema de tratamiento

## **Generación de un catálogo de medios físicos y electrónicos, a través de los cuales se obtienen los datos personales.**

Identificado el tratamiento de datos del cual está a cargo la unidad administrativa, se determinó lo siguiente, de acuerdo con el ciclo de vida de los datos personales:

- **Identificación de los medios de obtención de los datos personales y base de legitimación, conforme a la Ley para su tratamiento**

De manera enunciativa, se señalan diversas maneras por las cuales pueden obtenerse los datos personales:

- Directamente del titular
  - De manera presencial
  - Vía telefónica
  - Por correo electrónico
  - Por Internet o sistema informático
  - Por escrito presentado directamente en las oficinas de esta Fiscalía General de la República
  - Por escrito enviado por mensajería
- En su caso, mediante transferencia
  - Quién transfiere los datos personales y para qué fines
  - Medios por los que se realiza la transferencia
- De una fuente de acceso público
  - Bases de datos, sistemas o archivos que por disposición de ley puedan ser consultadas públicamente cuando no exista impedimento por una norma limitativa y sin más exigencia que, en su caso, el pago de una contraprestación, tarifa o contribución.

A partir de lo anterior, esta FGR cuenta con los inventarios de los distintos tratamientos de datos personales que realiza, identificando los elementos que señala el artículo 58 de los Lineamientos Generales y basados en el ciclo de vida de los datos personales, como lo establece el artículo 59 de los Lineamientos Generales.

Los inventarios forman parte integral del presente documento de seguridad y se encuentran contenidos en el **anexo I**, denominado **Inventario de Datos Personales y Sistemas**.

## **FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATEN DATOS PERSONALES**

Una vez desarrollado el inventario de datos personales y sistemas de tratamiento, se identificaron a las unidades administrativas que intervienen durante el procesamiento y aprovechamiento de los datos personales por cada sistema de datos identificado.

Lo anterior, con la finalidad de tener pleno conocimiento de quiénes tratan datos personales, y las actividades que realizan durante el tratamiento declarado.

Al respecto, resulta conveniente traer a colación lo establecido en el artículo 33, fracción II de la Ley General, el cual, dispone 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:*

*[...]*

*II. Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales;*

*[...]"*

Por su parte, el artículo 57 de los Lineamientos Generales, dispone 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, conforme a sus respectivas competencias, se requirió a las unidades administrativas llevaran a cabo la identificación de sus funciones y obligaciones, así como su intervención durante el ciclo de vida, contenido en el **anexo II**, denominado **Definición de funciones y obligaciones de los servidores públicos involucrados**.

## ANÁLISIS DE RIESGO

De conformidad con el artículo 33, fracción IV de la Ley General, el análisis de riesgo debe ser elaborado considerando las amenazas y vulnerabilidades existentes para los datos personales que son recabados y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, el tipo de hardware, software, o las características del responsable, entre otros.

Por su parte, el artículo 60 de los Lineamientos Generales, considera en la realización del análisis de riesgo lo siguiente:

- La existencia de requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico para proteger los datos personales.
- El valor de los datos personales de acuerdo con su clasificación previamente definida, y su ciclo de vida, de conformidad con la normatividad aplicable.
- El valor y exposición de los activos involucrados en su tratamiento.
- Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida.
- El riesgo inherente a los datos personales tratados, su sensibilidad (datos personales sensibles), el desarrollo tecnológico, las posibles consecuencias de una vulneración para los titulares, las transferencias de datos personales que se realicen, el número de titulares, las vulneraciones previas ocurridas en los sistemas de tratamiento, y 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; siempre en función y estricto apego a la normatividad aplicable.

En atención a lo anterior, las diversas unidades administrativas analizaron el riesgo existente en cada uno de los tratamientos de datos personales que realizan, considerando los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico, el valor de los datos personales de acuerdo con su clasificación previamente definida y su ciclo de vida, el valor y exposición de los activos involucrados en el tratamiento de los datos personales, así como las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida.

Con la información obtenida, la Unidad Especializada en Transparencia integró por cada unidad administrativa el análisis de riesgo respectivo, el cual se encuentra documentado a través del **anexo III**, denominado **Análisis de Riesgos**.

## ANÁLISIS DE BRECHA

Para la realización de este apartado se tomaron en consideración las medidas de seguridad existentes y efectivas, las medidas de seguridad faltantes, así como la existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.

Al respecto, de conformidad con lo estipulado en el artículo 33, fracción V de la Ley General, para establecer y mantener las medidas de seguridad para la protección de los datos personales, es necesaria la elaboración de un análisis de brecha en el que se comparen las medidas de seguridad existentes contra las faltantes.

Por su parte, el artículo 61 de los Lineamientos Generales, dispone que en la realización del análisis de brecha se debe considerar lo siguiente:

- Las medidas de seguridad existentes y efectivas.
- Las medidas de seguridad faltantes.
- La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.

De tal forma que, una vez identificados los riesgos y medidas de seguridad ineludibles, es procedente el análisis de brecha, en el que se identifiquen los controles que deben ser implementados.

Bajo esa directriz las unidades administrativas llevaron a cabo el análisis de las brechas atendibles identificando las medidas de seguridad con las que cuentan, las medidas de seguridad faltantes, así como la existencia de nuevas medidas de seguridad que pudieran reemplazar a uno o más controles implementados en la actualidad para que no suceda una vulneración a la seguridad de los datos personales, aspectos que se encuentran documentados a través del **anexo IV**, denominado **Análisis de Brecha**.

## PLAN DE TRABAJO

Se establecen las acciones a realizar para la protección de los datos personales conforme a los resultados del análisis de riesgos y análisis de brecha, para la implementación de las medidas de seguridad faltantes.

El artículo 33, fracción VI, de la Ley General, estipula que, para establecer y mantener las medidas de seguridad, se deberá 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.

Por su parte, el artículo 62 de los Lineamientos Generales, dispone que el Plan de Trabajo debe definir las acciones a implementar de acuerdo con el resultado del análisis de riesgo y brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer, considerando los recursos designados, el personal interno de la instancia y las fechas comprometidas para la implementación de las medidas de seguridad nuevas o faltantes.

Así, el Plan de Trabajo concentra los retos que en materia de seguridad de datos personales afrontan las unidades administrativas que identificaron un Sistema de tratamiento de datos, sustentado en el análisis de los riesgos y las medidas de seguridad que se estiman deben implementarse, en el contexto de organización interna y la evolución tecnológica de sus sistemas.

Al respecto, con apoyo de la Guía para la integración del documento de seguridad, relacionando el riesgo localizado y la brecha atendible, de cada tratamiento de datos personales las instancias determinaron lo siguiente:

- El mecanismo de control para atender la brecha identificada.
- El período de monitoreo.
- La fecha en que se implementará
- Evidencia entregable

Aspectos que se encuentran documentados a través de los archivos electrónicos que constituyen el **anexo V**, denominado **Plan de Trabajo**.

## LOS MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD.

Inicialmente, de conformidad con lo establecido en el artículo 30, fracción V, de la Ley General, se debe de establecer un sistema de supervisión y vigilancia, incluyendo auditorías, que permita comprobar el cumplimiento de las políticas de protección de datos personales.

Por su parte, 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 conformidad 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.*

*Aunado a lo previsto en las fracciones anteriores del presente artículo, el responsable deberá contar con un programa de auditoría, interno y/o externo, para monitorear y revisar la eficacia y eficiencia del sistema de gestión."*

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

En ese sentido, cada una de las unidades administrativas que llevan a cabo tratamientos de datos personales, elaboraran un reporte de sus inventarios en los que se sean precisadas las medidas de seguridad implementadas, las cuales se dividen en medidas físicas, técnicas y administrativas.

## PROGRAMA GENERAL DE CAPACITACIÓN

El artículo 30, fracción III de la Ley General, establece que entre los mecanismos que se deberán adoptar para cumplir con el principio de responsabilidad, se encuentra el poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales.

En ese sentido, con relación al programa de capacitación, el artículo 33, fracción VIII 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 efectuado.

Por su parte, el numeral 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:*

*Los requerimientos y actualizaciones del sistema de gestión;*

*La legislación vigente en materia de protección de datos personales y las mejores prácticas relacionadas con el tratamiento de éstos;*

*Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales, y*

*Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad."*

Al respecto, a propuesta de la Unidad Especializada en Transparencia, el Comité de Transparencia de esta Fiscalía General de la República llevará a cabo la aprobación del programa de capacitación de datos personales, de manera anual, mismo que se integrará a este documento como **anexo VI**.

## 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 mérito de lo anterior, la Unidad Especializada en Transparencia procederá a la elaboración de un proyecto de actualización del documento de seguridad cuando se materialicen los supuestos antes señalados.

En ese sentido, en caso de que ocurra alguna actualización al documento de seguridad, este tendrá que ser sometido a consideración del Comité de Transparencia para su actualización.