UNIVERSIDAD
DE LA SALUD

GUÍA

MEDIDAS DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES

Índice

03 Introducción

04 Glosario

06 Importancia de la Seguridad de los Datos Personales

07 Deber de los responsables

08 Medidas de Seguridad de los Datos Personales

13 Medidas de Seguridad Técnicas

14 Medidas de Seguridad Físicas

15 Medidas de Seguridad Administrativas

17 Vulneración a la Seguridad de los Datos Personales

19 Normativa Aplicable

Introducción

El presente documento, tiene por objeto orientar a los responsables del tratamiento de datos personales, con relación a la implementación de medidas de seguridad para la protección de datos personales, las cuales forman parte del sistema de gestión y documento de seguridad que, conforme a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, deberán establecer.

De igual forma es una herramienta que ayuda a los involucrados en el tratamiento de datos personales a implementar controles de seguridad desde los más sencillos y de fácil alcance, hasta los que sean necesarios para garantizar la protección de los datos personales.

El mantenimiento de forma segura de los sistemas, a través de los que se obtienen, almacenan, procesan y/o comparten datos personales, puede ser una tarea compleja, que requiere tiempo, conocimiento y recursos especializados. Sin embargo, esta tarea se facilita cuando quien trata datos personales identifica adecuadamente el uso de la información en cada uno de los procesos de su institución.

Glosario

01 **DERECHOS ARCO**

Acceso, rectificación, cancelación, oposición de datos personales.

02 **INSTITUTO**

Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México.

03 **LEY**

Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México.

04 **RESPONSABLE**

Cualquier sujeto obligado, que decida y determine finalidad, fines, medios, medidas de seguridad y demás cuestiones relacionadas con el tratamiento de datos personales. (art 3, fracción XXVIII LPDPPSOCDMX)

Glosario

05

TITULAR

La persona física a quien corresponden los datos personales

06

DATOS PERSONALES

Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona física es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información como puede ser nombre, número de identificación, datos de localización, identificador en línea o uno o varios elementos de la identidad física, fisiológica, genética, psíquica, patrimonial, económica, cultural o social de la persona

Importancia de la seguridad de los Datos Personales.

El derecho a la protección de datos personales, es la facultad que otorga la Ley para que los titulares, como dueños de sus datos personales, decidan a quiénes proporcionan su información, cómo y para qué. El ejercicio de este derecho permite que puedan acceder, rectificar, cancelar y oponerse al tratamiento de su información personal, y se le denomina Derechos ARCO.

Este derecho sirve para exigir un correcto tratamiento de la información personal proporcionada a los responsables.
Es importante la seguridad de los datos personales porque:

- La protección de datos personales es un derecho humano.
- Ayuda a prevenir y mitigar los efectos de una fuga y/o mal uso de los datos personales.
- Evita daños a la reputación e imagen de la institución.
- Evita sanciones a los servidores públicos.

El objetivo de implementar medidas de seguridad es, ayudar a reducir el riesgo de un incidente y sus consecuencias desfavorables. En caso de que se presente un incidente, se reduzca el daño a los titulares, así como a la institución.

Deber de los Responsables

En el tratamiento de datos personales que llevan a cabo los responsables, deberán observar los principios de: lealtad, consentimiento, calidad, licitud, finalidad, información, proporcionalidad y responsabilidad.

De igual manera deberán cumplir con dos deberes: el de confidencialidad y el de seguridad.

El deber de seguridad, señala que con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá 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, así como garantizar su confidencialidad, integridad y disponibilidad.

La seguridad de los datos personales se basa en tres pilares fundamentales:

- Confidencialidad (para la persona correcta),
- Integridad (información correcta) y,
- Disponibilidad (en el momento correcto).

El documento de seguridad es el instrumento en el que los responsables describen y dan cuenta de manera general, sobre las medidas de seguridad, técnicas, físicas y administrativas adoptadas para garantizar precisamente esos tres pilares de la seguridad.

Medidas de seguridad de los Datos Personales

Los responsables del tratamiento de datos personales deberán establecer e implementar medidas de seguridad para la protección de la información personal que poseen, y estas forman parte del sistema de gestión de datos personales.

La legislación en la material, define las **medidas de seguridad** como: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales y los sistemas de datos personales

Las medidas de seguridad adoptadas por el responsable de acuerdo al artículo 25 de la Ley :

I) El riesgo inherente a los datos personales tratados.
Entendido como el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales para una tercera persona no autorizada para su posesión o uso en función de la sensibilidad de éstos; las categorías de titulares; el volumen total de los datos personales tratados; la cantidad de datos personales que se tratan por cada titular; la intensidad o frecuencia del tratamiento, o bien, la realización de cruces de datos personales con múltiples sistemas o plataformas informáticas.

II) La sensibilidad de los datos personales tratados.
Cuando se traten datos personales sensibles, a los que se refiere el artículo 3, fracción X de la Ley, entendidos como: 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, información biométrica, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;

III**) El desarrollo tecnológico.**
Resulta importante considerar el desarrollo tecnológico para la adopción de medidas de seguridad de los datos personales, que resulten eficientes y garanticen la integridad, disponibilidad y confidencialidad de estos.

IV**) Las posibles consecuencias de una vulneración para los titulares**.
Al crear e implementar medidas de seguridad, es sustancial considerar las posibles vulneraciones que se pudieran presentar en cualquier fase del tratamiento de los datos personales, y las consecuencias que esto traería a los titulares de los datos personales. Vulneraciones a la seguridad de los datos que pudieran comprometer de manera significativa los derechos patrimoniales o morales de las personas.

V) Las transferencias de datos personales que se realicen.
Son cualquier comunicación de datos personales, dentro o fuera del territorio mexicano, realizada a persona distinta del titular, responsable o encargado, considerando con especial énfasis:

- Las finalidades que motivan éstas y su periodicidad prevista;
- Las categorías de titulares;
- La categoría y sensibilidad de los datos personales transferidos;
- El carácter nacional, o en su caso internacional de los destinatarios o terceros receptores y la tecnología utilizada para la realización de éstas;
- Entre otros.

VI**) El número de titulares.**
Es importante que el responsable, considere el número de titulares de los que trata su información personal, conforme a las atribuciones que le han sido conferidas, en la adopción de medidas de seguridad, para la protección de dicha información.

VII**) Las vulneraciones previas ocurridas en los sistemas de tratamiento.**
Se deberá contemplar las incidencias o vulneraciones previas que se hayan presentado respecto al sistema de tratamiento de datos personales, esto con la finalidad de implementar y adoptar medidas de seguridad eficientes que eviten la repetición de vulneraciones a la información personal que se posee de los titulares.

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.

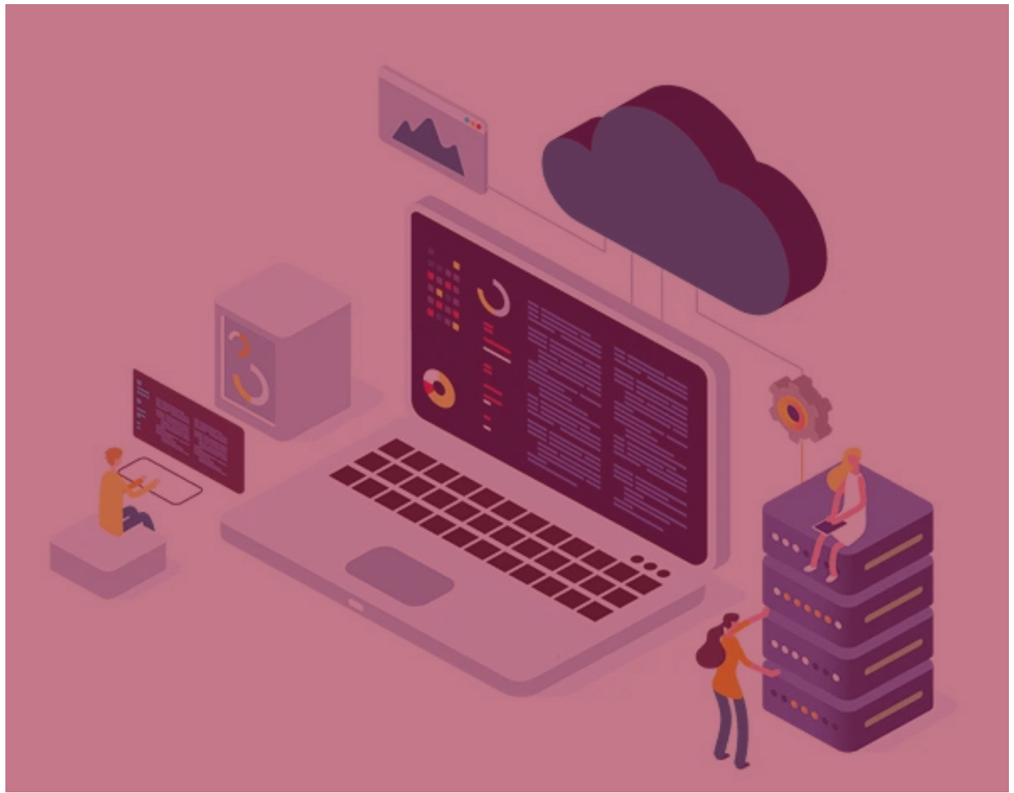
El análisis que se haga de los datos personales no debe ser únicamente en su volumen, sino en el riesgo de la reputación de los titulares afectados.

Para establecer y mantener las medidas de seguridad en la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes acciones:

- 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.
- Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales.
- Elaborar un inventario de datos personales y de los sistemas de tratamiento.
- 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: hardware, software, personal del responsable, entre otros.
- Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable.
- 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.

- Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están expuestos los datos personales.
- 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.

Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenida en un sistema de gestión.



Medidas de Seguridad Técnicas

Son el 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 consideran 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

Medidas de Seguridad Físicas

Son el 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 consideran 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 Administrativas

Estas medidas se refieren a las 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;

Dentro de las medidas de seguridad administrativas, se encuentran las siguientes:

- **Política de seguridad.**

Definición de directrices estratégicas en materia de seguridad de activos, alineadas a las atribuciones de las dependencias o entidades. Incluye la elaboración y emisión interna de políticas, entre otros documentos regulatorios del sujeto obligado.

- **Cumplimiento de la normatividad.**

Los controles establecidos para evitar violaciones a la normatividad vigente, o la política de seguridad interna u obligaciones contractuales. Abara , entre otro s , e l c u m p l i m i e n to y l a identificación de requerimientos tales como la legislación aplicable al sujeto obligado, los derechos de propiedad intelectual, la protección de datos personales y la privacidad de la información personal.

- **Organización de la seguridad de la información.**

Establecimiento de controles internos y externos a través de los cuales se gestione la seguridad de activos. Considera la organización interna, que a su vez se refiere al compromiso de la alta dirección y la designación de responsables, entre otros objetivos; asimismo, considera aspectos externos como la identificación de riesgos relacionados con terceros.

- **Clasificación y control de activos.**

Establecimiento de controles en materia de identificación, inventario, clasificación y valuación de activos conforme a la normatividad aplicable.

- **Seguridad relacionada a los recursos humanos.**

Controles orientados a que el personal conozca el alcance de sus responsabilidades respecto a la seguridad de activos, antes, durante y al finalizar la relación laboral.

- **Administración de incidentes.**

Implementación de controles enfocados a la gestión de incidentes presentes y futuros que puedan afectar la integridad, confidencialidad y disponibilidad de la información. Incluye temas como el reporte de eventos y debilidades de seguridad de la información.

- **Continuidad de las operaciones.**

Establecimiento de medidas con el fin de contrarrestar las interrupciones graves de la operación y fallas mayores en los sistemas de información. Incluye la planeación, implementación, prueba y mejora del plan de continuidad de la operación del sujeto obligado.

Vulneración a la Seguridad de los Datos Personales

La vulneración tiene lugar cuando, intencionada o no intencionadamente, se liberan datos personales en un ambiente no confiable. Puede ocurrir en cualquier fase del tratamiento de datos y podría afectar los derechos patrimoniales o morales de los titulares.

Los tipos de vulneraciones que pueden ocurrir pueden ser (Art. 31 de la Ley):

a) Pérdida o destrucción no autorizada.
b) Robo, extravío o copia no autorizada.
c) Uso, acceso o tratamiento no autorizado.
d) Daño, alteración o modificación no autorizada.

Obligaciones por la vulneración a la seguridad de los datos personales.

La Ley establece que en caso de que ocurra una vulneración a la seguridad de los datos personales, que afecten de forma significativa los derechos personales y patrimoniales de los titulares, el responsable está obligado a comunicar tal situación al titular y al Instituto, sin dilación alguna, en cuanto tenga confirmado que dicha vulneración en verdad ocurrió.

Concretamente, el responsable deberá informar (Art. 34 de la Ley):

- La naturaleza del incidente.
- Los datos personales comprometidos.
- Las recomendaciones que el titular puede adoptar para protegerlos.
- Las acciones correctivas realizadas de forma inmediata.
- Los medios donde podrá obtener más información al respecto.

La Ley señala, además, que el responsable debe llevar una bitácora en la que describa las vulneraciones de seguridad ocurridas en su institución. En ella se tiene que registrar:

- Fecha en que ocurrió la vulneración.
- Motivo de la vulneración.
- Acciones correctivas implementadas, de forma inmediata y definitiva.

Marco Normativo

- LEY DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DE LA CIUDAD DE MÉXICO
- LINEAMIENTOS GENERALES SOBRE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DE LA CIUDAD DE MÉXICO