Órgano Constitucional Autónomo

Núm. 18 Año VI Victoria de Durango, 30 de octubre de 2020

# Gaceta Institucional

## Contenido

# *GUÍA DE MEDIDAS DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES*

## 1. GLOSARIO DE TÉRMINOS.

**Derechos ARCO:** Acceso, rectificación, cancelación, oposición de datos personales.

**Instituto:** Instituto Duranguense de Acceso a la Información Pública y de Protección de Datos Personales.

**Ley:** Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Durango.

**Responsable:** Los sujetos obligados señalados en el artículo 1, párrafo 5, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Durango.

## 2. 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 del Estado de Durango, 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, recursos y conocimientos 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.

## 3. 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.

## 4. 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.

## 5. 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 materia, tanto nacional, como local, define las medidas de seguridad como: el conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.

Las medidas de seguridad adoptadas por el responsable deberán considerar:

**a) 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.

**b) La sensibilidad de los datos personales tratados.**

Cuando se traten datos personales sensibles, a los que se refiere el artículo 3, fracción XI 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 un riesgo grave. 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, preferencia sexual, entre otros.

**c) 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.

**d) 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.

**e) 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.

**f) 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.

**g) 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.

**h) 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 contenidas en un sistema de gestión.

## 6. 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 recursos involucrados en su tratamiento. 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.

**e)** Entre otras.

***Las medidas de seguridad técnicas*** son las aplicables a sistemas de datos personales en soportes electrónicos, servicios e infraestructura de telecomunicaciones y tecnologías de la información, en las que se podrán prever las siguientes acciones:

- **Gestión de comunicaciones y operaciones.** Es establecer controles orientados a definir la operación correcta y segura de los medios de procesamiento de información, tanto para la gestión interna, como la que se lleva a cabo con terceros. Incluye, entre otros aspectos, protección contra código malicioso y móvil, copias de seguridad, gestión de la seguridad de redes y manejo de medios de almacenamiento.

- **Control de acceso**. Se deberá establecer medidas para controlar el acceso a la información, activos e instalaciones por parte de los responsables autorizados para tal fin, considerando en ello, la protección contra la divulgación no autorizada de información. Abarca, entre otros temas, gestión de acceso de los usuarios, control de acceso a redes, control de acceso a sistemas operativos y control de acceso a las aplicaciones y a la información.

- **Adquisición, desarrollo, uso y mantenimiento de sistemas de información.** Relativo a la Integración de controles de seguridad a los sistemas de información, desde su adquisición o desarrollo, durante su uso y mantenimiento, hasta su cancelación o baja definitiva. Considera el procesamiento adecuado en las aplicaciones, controles criptográficos y seguridad de los archivos de sistema, entre otros.

## 7. 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.

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 las instalaciones de la organización; y

**d)** Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz que asegure su disponibilidad, funcionalidad e integridad.

## 8. 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, formación 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 de la normatividad vigente, o la política de seguridad interna u obligaciones contractuales. Abarca, entre otros, el cumplimiento y la 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, entre otros aspectos, 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.

## 9. 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:

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.

e) Entre otros.

### 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:

- 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.

**DATOS DE CONTACTO DEL IDAIP.**

**Domicilio:** Calle Negrete número 807, C.P. 34000, Zona Centro, de esta Ciudad de Durango, Dgo.
**Página de Internet:** www.idaip.org.mx
**Teléfono de contacto:** 618 811 77 12
**Horario de atención:** de 08:00 a 16:00 horas.
**Correo electrónico de atención:** buzon@idaip.org.mx

## Órgano Constitucional Autónomo

### CONSEJO GENERAL

Alma Cristina López de la Torre, Comisionada Presidente
Paulina Elizabeth Compean Torres, Comisionada Propietaria
Luz María Mariscal Cárdenas, Comisionada Propietaria

Juan Carlos Rodríguez Rosales, Titular del Órgano de Control Interno
Omar Ivan Quiñones Valdez, Titular de la Unidad de Transparencia
Luciano Valenzuela García, Encargado de Comunicación Social

---

Antonio Leonel Ayala Valdez, Secretario Ejecutivo

Julia Elena Sánchez Solís, Coordinadora Administrativa
José Alejandro Guerrero Murga, Coordinador de Verificación, Seguimiento y Evaluación a Sujetos Obligados
Armando Espinosa Aguilera, Coordinador de Capacitación y Cultura de la Transparencia
Pablo Ignacio Gómez Martínez, Coordinador de Promoción y Vinculación
Guillermo Alvarado Montañez, Coordinador de Sistemas

---

Eva Gallegos Díaz, Secretaria Técnica

Mario Alonso Medrano Romero, Coordinador Jurídico
Cecilia Loera Domínguez, Coordinadora de Protección de Datos Personales
Gema Ruvalcaba Ochoa, Encargada de la Coordinación de Gobierno Abierto y Transparencia Proactiva
Natalia Franco Soler, Encargada de la Coordinación de Equidad de Género e Inclusión Social

La Gaceta Institucional es el órgano oficial de difusión del Instituto Duranguense de Acceso a la Información Pública y de Protección de Datos Personales (IDAIP), según lo dispone el artículo 11 del Reglamento Interior del propio órgano garante, su distribución es gratuita y se puede consultar la versión digital en www.idaip.org.mx

Calle Negrete 807 Oriente, C.P. 34000 Durango, Dgo.
Teléfonos: 618-811-77-12 y 01800-581-72-92