Instituto de Acceso a la Información Pública del Distrito Federal

MANUAL DE AUTOFORMACIÓN SOBRE

LA LEY DE PROTECCIÓN DE DATOS PERSONALES PARA EL DISTRITO FEDERAL

INSTITUTO DE ACCESO A LA INFORMACIÓN PÚBLICA DEL DISTRITO FEDERAL

COLECCIÓN CAPACITACIÓN A DISTANCIA

05

Colección Capacitación a Distancia
05

MANUAL DE AUTOFORMACIÓN SOBRE LA LEY DE PROTECCIÓN DE DATOS PERSONALES PARA EL DISTRITO FEDERAL

Instituto de Acceso a la Información Pública del Distrito Federal

DIRECTORIO

AUTORA DEL TEXTO
Mariana Cendejas Jáuregui

COORDINACIÓN
Ma. de los Ángeles Hernández Sánchez
Directora de Capacitación y Cultura
de la Transparencia

EQUIPO TÉCNICO
Sonia Barrera García
Dulce Ma. Jara Reyes

DR © 2009, Instituto de Acceso a la Información Pública del Distrito Federal.
Dirección de Capacitación y Cultura de la Transparencia.
La Morena No. 865, Local 1, Col. Narvarte Poniente,
Del. Benito Juárez, C. P. 03020, México, Distrito Federal.
“Plaza de la Transparencia”.
Primera edición, diciembre de 2009.
ISBN: 978-607-95070-0-8.

Ejemplar de distribución gratuita.
Prohibida su venta.
Impreso y hecho en México.

Fotografía de familia en portada: Benjamin Earwicker.

Índice

Índice

Presentación

En la mayoría de las relaciones que se establecen en una comunidad, se requiere del intercambio de información relacionada con nuestra persona. En el trabajo, en nuestras relaciones personales, para la obtención de bienes y servicios, en la realización de trámites ante las autoridades, entre otros, requerimos proporcionar o intercambiar datos, que nos identifican y que se relacionan con nuestra vida privada.

El intercambio de gran cantidad de datos personales que circulan a través de esta serie de transacciones cotidianas que realizamos, se ha potenciado con el uso de tecnologías de la información, por ejemplo, la internet, cuyo crecimiento ha permitido la obtención y transmisión de grandes bases de datos que almacenan información sobre la vida privada de las personas.

El almacenamiento masivo de información que concierne a las personas, permite potencialmente, la creación de perfiles que pueden emplearse para un uso diferente para el que fueron proporcionados originalmente o darles un uso inadecuado y con ello provocar injerencias arbitrarias o ilegales en la vida privada, lo que evidencia una nueva amenaza para los derechos de las personas.

Esta situación, ha generado una nueva interpretación de los derechos y libertades de las personas que contempla esta realidad. Por ello, algunas de las legislaciones nacionales y también supranacionales, se dieron a la tarea de reforzar las garantías de los ciudadanos

frente a esta amenaza tecnológica que permite con mayor rapidez y eficiencia, la creación e intercambio de bases de datos, lo que ha dado como resultado que la protección de datos personales haya cobrado mayor relevancia, sobre todo, a través de la promulgación de leyes en la materia.

La intención de estas normas no es impedir o dificultar la actividad informática, fundamental para el desarrollo, sino conciliar el avance tecnológico con la protección y tutela de los derechos y libertades de las personas.

En México, nuestra Carta Magna establece que, “nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones…”, con base en este mandato, se dio inicio a la regulación de los datos que, sobre las personas, posee el gobierno para el desarrollo de sus funciones.

Debemos precisar que la reforma de 2007 al artículo 6º constitucional contiene una referencia expresa a los datos personales como límite al derecho de acceso a la información pública y que las recientes reformas a los artículos 16 y 73 de nuestra Carta Magna, dotan de autonomía y constitucionalidad al derecho a la protección de datos personales, por un lado, y, por otro, otorgan de facultades expresas al Congreso de la Unión para legislar en materia de protección de datos personales en posesión de entidades privadas.

A nivel federal, hasta ahora carecemos de una ley específica que regule la protección de datos personales en posesión tanto de entidades públicas como privadas, aunque existen disposiciones que se encuentran dispersas en diversos ordenamientos jurídicos, en particular la Ley Federal de Transparencia y Acceso a la Información Pública, que en su Capítulo IV, regula diferentes aspectos que garantizan a los ciudadanos la protección de sus datos personales en el ámbito de las entidades gubernamentales de la Federación.

A nivel estatal, Guanajuato y Oaxaca tienen leyes específicas en la materia que son aplicables solamente a entes de derecho público y en el caso de Morelos existe una Ley de Información Pública, Estadística y Protección de Datos Personales, que al igual que las anteriores, no es aplicable a entes de derecho privado.

Una cuestión que vale la pena destacar es que la única ley específica en la materia aplicable tanto al sector público como al privado es la de Colima, la cual otorga protección a los datos personales en posesión de estos sectores dentro de dicho Estado.

En el caso específico de la Ciudad de México, que es el que nos ocupa en este manual, el 3 de octubre de 2008, se publicó en la Gaceta Oficial del Distrito Federal, la Ley de Protección de Datos Personales para el Distrito Federal (LPDPDF). Esta Ley, se orienta a la regulación de los entes públicos, entendidos éstos como todas aquellas instituciones que conforman los tres niveles de gobierno, además, los partidos políticos, asociaciones y agrupaciones políticas; así como aquellos que la legislación local reconozca como de interés público y ejerzan gasto público; y los entes equivalentes a personas jurídicas de derecho público o privado, ya sea que en ejercicio de sus actividades actúen en auxilio de los órganos antes citados o ejerzan gasto público:

La Asamblea Legislativa del Distrito Federal; el Tribunal Superior de Justicia del Distrito Federal; el Tribunal de lo Contencioso Administrativo del Distrito Federal; el Tribunal Electoral del Distrito Federal; el Instituto Electoral del Distrito Federal; la Comisión de Derechos Humanos del Distrito Federal; la Junta de Conciliación y Arbitraje del Distrito Federal; la Jefatura de Gobierno del Distrito Federal; las Dependencias, Órganos Desconcentrados, Órganos Político Administrativos y Entidades de la Administración Pública del Distrito Federal; los Órganos Autónomos por Ley.

Es así que, los entes públicos del Distrito Federal, están obligados, en principio, a garantizar la confidencialidad de los datos personales que tienen sobre las personas que atienden, por lo que el tratamiento y gestión de este tipo de información debe ser, a partir de la promulgación de esta Ley, bajo los mecanismos y disposiciones que este ordenamiento mandata.

Además de esta Ley, el Distrito Federal cuenta con “Lineamientos para la Protección de Datos Personales en el Distrito Federal” que fueron aprobados por el Pleno del Instituto de Acceso a la Información Pública del Distrito Federal (InfoDF) y publicados en la Gaceta Oficial el 26 de octubre de 2009. Su finalidad es fortalecer el marco normativo en materia de datos personales y establecer las directrices y criterios

para la aplicación e implementación de la Ley de Protección de Datos Personales para el Distrito Federal.

En este ordenamiento, se establecen: definiciones de conceptos del derecho de protección de datos personales; se hace referencia a los sistemas, a la seguridad y tratamiento de los datos personales, así como a las obligaciones de los sujetos obligados en esta materia; se señalan también, las atribuciones con que cuenta el InfoDF para garantizar el cumplimiento de la LPDPDF por parte de los entes públicos, y se establece el procedimiento al que deberán sujetarse tanto particulares como los sujetos obligados en el ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO).

Para avanzar en esta ruta, el Instituto de Acceso a la Información Pública del Distrito Federal, pone a su disposición este manual de autoformación a distancia como una más de las alternativas de capacitación sobre la Ley y los Lineamientos existentes en materia de Protección de Datos Personales para el Distrito Federal. Se trata de una valiosa herramienta de autoformación, que le permitirá conocer de manera simplificada estos ordenamientos, mediante explicaciones puntuales sobre su historia, su estructura, su marco de aplicación, sus límites y sus posibilidades.

El propósito fundamental del Instituto es ofrecerle un instrumento de capacitación que usted mismo pueda administrar, razón por la cual decidimos aprovechar las ventajas de la formación autodidacta. Ésta es, sin duda, una modalidad en la que usted gozará de entera libertad para avanzar a su propio ritmo en el proceso de aprendizaje. Usted decide cuándo comienza y cuándo termina.

El contenido del manual de autoformación está organizado en tres módulos, el primero le aportará un panorama general sobre los conceptos más importantes que están alrededor del derecho a la protección de datos personales; en el segundo, encontrará información sintética sobre el desarrollo de algunas legislaciones en materia de protección de datos personales en el contexto mundial, así como una breve reseña histórica de la promulgación de la Ley y los Lineamientos en el Distrito Federal; y en el módulo tercero se abordarán los aspectos más relevantes contenidos en ambos ordenamientos.

Esperamos que este manual de autoformación le sea útil a la población para comprender la importancia que tiene el derecho a la protección de datos personales, como una condición para garantizar su derecho a la privacidad, y que a los servidores públicos, les motive a emprender los cambios que requiere realizar la Administración Pública para garantizar a la población la protección y el correcto tratamiento de sus datos personales.

Objetivos de aprendizaje

Al concluir el Manual el participante podrá:

- Comprender la importancia de la protección de los datos personales como una condición que contribuye a garantizar el derecho a la privacidad de las personas.
- Identificar los conceptos y definiciones básicas que inspiraron la aprobación de leyes de protección de datos personales.
- Tener un conocimiento general de los aspectos más relevantes que establecen la ley y los lineamientos de datos personales en el D. F. en sus diferentes títulos y capítulos.
- Consultar de forma directa los textos de la Ley y los Lineamientos como apoyo para cualquier proceso relacionado con la protección de datos personales y el ejercicio de sus derechos ARCO, ya sea como servidor público o como persona interesada en el tema.

Guía del participante

Lea la guía completa antes de iniciar

Bienvenido al *Manual sobre la Ley de Protección de Datos Personales para el Distrito Federal*.

La estructura del manual responde a un plan conductor del aprendizaje que no exige al participante acudir a recursos externos o de mayor profundidad. Es un documento completo con toda la información que requieres para la comprensión de la temática expuesta.

Quizá seas un servidor público del Gobierno del Distrito Federal, miembro de alguna organización de la sociedad civil o una persona que necesita saber cómo acceder a la información que sobre su persona tiene el gobierno local.

Cualquiera que sea tu caso, te aseguramos que este manual te ayudará a comprender o a encauzar de mejor manera tus necesidades e inquietudes.

Te sugerimos que antes de iniciar su capacitación leas cuidadosamente la Presentación, los Objetivos de aprendizaje del manual y la presente Guía del participante, esto te ayudará significativamente a conducir tu estudio con mayor efectividad.

Estructura del Manual

Para facilitar su estudio, el manual está estructurado en tres unidades de aprendizaje que denominamos módulos:

El **Módulo uno**, Conceptos y Definiciones Básicas, explica en cuatro temas los conceptos de derecho a la intimidad, derecho a la privacidad, datos personales y protección de datos personales.

El **Módulo dos**, Antecedentes de las Leyes de Protección de Datos Personales, expone en tres temas las ideas básicas sobre la institucionalización del derecho de protección de datos personales, así como una reseña histórica sobre la Ley de Protección de Datos Personales para el D. F.

El **Módulo tres**, Aspectos Relevantes de la Ley de Protección de Datos Personales para el Distrito Federal, entra de lleno en todos los aspectos de la Ley. Incluye 11 temas, a saber:

1) La Protección de Datos Personales en el D. F.
2) Definiciones.
3) Principios.
4) Sistemas de Datos Personales.
5) Medidas de Seguridad.
6) Tratamiento de Datos Personales.
7) Obligaciones de los Entes Públicos.
8) Instituto de Acceso a la Información Pública del Distrito Federal.
9) Derechos ARCO y Procedimiento para su Ejercicio.
10) Recurso de Revisión.
11) Infracciones.

Estructura de los Módulos

Así se dividen los temas en los módulos:

- **Título del tema**, que te servirá como referencia para identificar la temática específica que se tratará.
- **Introducción**, que te ayudará a prever los conceptos por estudiar en el tema, entender la continuidad con respecto al anterior y prepararte para los contenidos que seguirán.
- **Objetivos**, que mostrarán de manera puntualizada los objetivos de aprendizaje por alcanzar cuando finalice el estudio del tema.
- **Desarrollo del tema**, donde hallarás explicados, definidos y hasta ejemplificados cada uno de los aspectos a que hace referencia el tema para alcanzar el objetivo de aprendizaje trazado.
- **Esquemas e infografía**, en cada tema encontrarás ilustraciones, gráficos y cuadros que te servirán para comprender de una sola vista los conceptos fundamentales del tema y los procesos más importantes a los que se refiere la Ley.
- **Síntesis**, que te servirá como recapitulación de lo visto en el tema, con el fin de prepararlo para su paso al siguiente tema de estudio y ofrecerle una última base para la autoevaluación.
- **Autoevaluación**, constituida por diversos tipos de cuestionarios en los que podrás verificar, mediante el método de pregunta y respuesta, los conocimientos adquiridos en cada uno de los módulos.
- **Referencias Bibliográficas**, que en su conjunto te ofrecen una pequeña colección de lecturas recomendadas para profundizar en el estudio de los temas relacionados con la protección de los datos personales.

Finalmente te presentamos un grupo de anexos que incluye, entre otros temas, una relación de entes públicos, un glosario de términos y el texto íntegro de la Ley de Protección de Datos Personales para el Distrito Federal y de los Lineamientos.

Recomendaciones de estudio

Éste es un manual muy sencillo, breve y puntual en sus exposiciones. Sin embargo, te sugerimos tener en cuenta las siguientes recomendaciones de uso:

1. El aprendizaje depende de ti exclusivamente.

No debes olvidarlo, ya que no dispondrás de tutor o guía a lo largo del curso. Más que una desventaja, esta ausencia te representa un enorme beneficio, pues podrás:

- ❒ Estudiar a tu propio ritmo.
- ❒ Dedicarle al estudio el tiempo que dispongas.
- ❒ Estudiar donde te plazca y cuando puedas.
- ❒ Repasar una y otra vez los temas.
- ❒ Motivarte a consultar información adicional.
- ❒ Resolver las autoevaluaciones cuantas veces sea necesario, hasta que estés satisfecho con tu aprendizaje.

2. Analiza el siguiente orden de estudio y si te resulta útil aplícalo.

1. *Lee la introducción del tema que vayas a estudiar.*
2. *Da un vistazo a cada uno de los esquemas. Trata de comprenderlos aún sin haber leído el texto.*
3. *Lee con calma el texto de desarrollo del tema. Continúa la lectura hasta que comprendas a cabalidad los párrafos leídos.*
4. *Anota los puntos más importantes de cada tema. Reflexiona sobre ellos antes de continuar.*
5. *Autoevalúate con los cuestionarios que incluimos.*

Cuando hayas cubierto el estudio de todos los temas y alcanzado todos los aciertos en todas las autoevaluaciones, entonces habrás concluido este curso-manual.

¡Felicidades!

Si ya concluiste el curso a través de este Manual de Autoformación y deseas obtener una Constancia de Acreditación validada por el InfoDF, puedes presentar tus evaluaciones a través del Aula Virtual de Aprendizaje (AVA), localizada en la página de internet www.aula-infodf.org/aulavirtual/. Una vez que hayas concluido las evaluaciones correspondientes a este curso, con las calificaciones requeridas (10 en cada tema), el InfoDF te otorgará la Constancia de Acreditación correspondiente. Para cualquier duda a este respecto, puedes comunicarte al 56 36 21 20 Ext. 159.

RECOMENDACIONES DE ESTUDIO

Conceptos y Definiciones Básicas

Módulo uno

Temario

1. Derecho a la Intimidad
2. Derecho a la Privacidad
3. ¿Qué es un Dato Personal?
4. Protección de Datos Personales

Introducción

Comenzaremos nuestro manual con el análisis de los conceptos que están directamente relacionados con las Leyes de Protección de Datos Personales y que constituyen un elemento fundamental para el entendimiento de las disposiciones que contienen, pero más allá de esto, dichos conceptos nos dan elementos para entender por qué la facultad de decidir sobre el manejo y control de la información que nos concierne, juega un papel fundamental en las democracias modernas.

En el tema que nos ocupa, que es el estudio de la Ley de Datos Personales para el Distrito Federal (LPDPDF) y sus Lineamientos, unificar criterios sobre cada uno de los conceptos a que hacen referencia estos ordenamientos, constituye un punto de partida obligado para clarificar de mejor manera, el abanico de obligaciones y derechos que nos ofrecen a los ciudadanos y a los servidores públicos.

El presente módulo abordará los siguientes temas:

1) Derecho a la Intimidad.
2) Derecho a la Privacidad.
3) ¿Qué es un Dato Personal?
4) Protección de Datos Personales.

Contenido del Módulo Uno

Objetivos del Módulo

Al final del módulo los participantes podrán:

- ❒ Conocer y explicar en qué consiste el derecho a la protección de datos personales teniendo una idea clara de lo que constituye el concepto de dato personal.
- ❒ Reflexionar sobre algunos conceptos directamente relacionados con la protección de datos personales que le conciernen e interesan a lo largo de toda su vida.

Tema 1. Derecho a la Intimidad

La palabra intimidad, de acuerdo con el diccionario de la Real Academia Española, se refiere a "la zona espiritual, íntima y reservada de una persona o de un grupo, especialmente de una familia". Es decir, apunta a la esfera personal de cada persona, en donde se encuentran los valores humanos y personales. La intimidad es un ámbito que debe estar reservado a la curiosidad de los demás contra intromisiones e indiscreciones ajenas.

Entendamos entonces como "intimidad" a aquella esfera personal y privada en la que se encuentran comportamientos, acciones y expresiones que no deseamos que lleguen al conocimiento público.[1]

La intimidad, en una sociedad democrática, es considerada como uno de los derechos fundamentales necesitados de protección. No sólo porque significa una barrera a la intromisión del Estado sino, también, porque permite el desarrollo íntegro de la personalidad de los ciudadanos.

Se dice que el respeto a la intimidad en un Estado de derecho es uno de los valores supremos en la convivencia social. En este sentido, resultan ilustrativas las palabras formuladas por el presidente del Tribunal Europeo de Derechos Humanos, quien afirmó que:

Aunque hablamos de protección de datos, de legislación de protección de datos y de Autoridades de protección de datos, no deben existir dudas respecto a la verdadera naturaleza del objetivo que motiva la creación de las normas de protección de datos o de las instituciones

que garantizan el cumplimiento de las mismas. Su finalidad real no es tanto la protección de datos sino la protección de las personas: más precisamente aún, es la protección de la vida privada de las personas en una nueva era que impone la recogida y almacenamiento de más y más datos sobre sus vidas privadas y hace aumentar las posibilidades de manipulación y mal uso de tales datos.[2]

El derecho a la intimidad, en su sentido amplio, se compone de una fase negativa (pasiva) que consiste en el derecho del individuo a ser dejado sólo, a vivir en paz y en soledad; y, de una fase positiva (activa), constituida por el principio de autodeterminación informativa o de poder de control sobre los datos personales.

La privacidad garantiza el círculo de exclusión del conocimiento ajeno y de la intromisión de terceros en el ámbito reservado de las personas

Definir y demarcar el contenido de este derecho no es tarea fácil y, la forma de protegerlo es todavía más compleja si se visualiza dentro de la "sociedad de la información" en la que se convive actualmente. Dicho ambiente informativo produce riesgos imprevisibles de manera continua que condenan a la ciencia del derecho a permanecer rezagada detrás de la tecnología y dificultan una concepción unívoca o estática de la intimidad.

No obstante, se puede definir como aquel derecho de la personalidad (con todo lo que denotan las características de este tipo de derechos) que brinda la facultad jurídica de excluir cualquier actividad de otro, que implique imposición, intromisión, injerencia y otras turbaciones, en los asuntos de la vida íntima del sujeto.

La intimidad se configura como derecho de "dentro hacia fuera", el derecho que asiste a toda persona para comunicar o no comunicar, a quien quiera, partes de su vida o de su pensamiento.[3]

Tema 2. Derecho a la Privacidad

¿A que nos referimos cuando hablamos de privacidad?

La privacidad constituye un conjunto más amplio, más global de facetas de nuestra personalidad que, aisladamente consideradas, pueden carecer de un significado intrínseco pero que, coherentemente enlazadas entre sí, arrojan un retrato de nuestra personalidad que tenemos derecho a mantener reservada.

Se refiere a toda aquella información y actividades en las cuales el Estado sólo puede intervenir para garantizar que se respeten nuestros derechos individuales y únicamente a petición *de parte*; este tipo de información hace referencia a nuestra vida privada o datos personales de forma genérica, por ejemplo, domicilio, teléfono, correo electrónico, edad, entre otros. Esta información, como veremos más adelante, tiene distintos niveles de protección por las leyes para que no sea difundida sin nuestra autorización.

Datos personales: toda información numérica, alfabética, gráfica acústica o de cualquier otro tipo concerniente a una persona física identificada o identificable

La privacidad, en definitiva, garantiza el círculo de exclusión del conocimiento ajeno y de la intromisión de terceros en el ámbito reservado de las personas: no constituye una mera oposición a la publicidad, sino una verdadera inmunidad a toda injerencia en los hechos relativos a uno mismo que no haya sido consentida.

Tema 3. ¿Qué es un Dato Personal?

Un elemento fundamental en los derechos que hemos analizado hasta aquí, es la identificación clara y precisa de lo que debemos entender por “dato personal”, ya que a través de ellos es que se podrían o no vulnerar nuestros derechos a la intimidad y privacidad.

Un dato personal es toda aquella información que pueda vincularse a un individuo. Las leyes sobre esta materia suelen definir a los datos personales como cualquier información relativa a una persona física identificada o identificable, considerándose identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, psíquica, económica, cultural o social.[4]

Así pues, cuando hablamos de “datos personales” nos estamos refiriendo a toda aquella información que se relaciona con nuestra persona y que nos identifica o nos hace identificables. Entre otras cosas, nos dan identidad, nos describen, precisan nuestro origen, edad, lugar de residencia, trayectoria académica, laboral o profesional. También describen aspectos más sensibles o delicados, como es el caso de nuestra forma de pensar, estado de salud, características físicas, ideología o vida sexual, entre otros.

Una definición clara sobre lo que debemos entender como “datos personales” y que será nuestra referencia en este Manual, la podemos encontrar en la Ley de Protección de Datos Personales para el Distrito Federal (LPDPDF). Esta Ley, tiene como objetivo, establecer los principios, derechos, obligaciones y procedimientos que regulan la protección y tratamiento de los datos personales en posesión de los entes públicos del Distrito Federal:

> **Datos personales**: toda información numérica, alfabética, gráfica acústica o de cualquier otro tipo concerniente a una persona física identificada o identificable. Tal y como son, de manera enunciativa y no limitativa: el origen étnico o racial, características físicas, morales o emocionales, la vida afectiva y familiar, el domicilio y teléfono particular, correo electrónico no oficial, patrimonio, ideología y opiniones políticas, creencias, convicciones religiosas y filosóficas, estado de salud, preferencia sexual, la huella digital, el ADN y el número de seguridad social, y análogos.

Como vemos, en esta definición se incluye toda aquella información que se relaciona con una persona y que a través de ella se le puede reconocer como por ejemplo, el nombre, firma, huella, fotografías, imágenes de vídeo e incluso grabaciones sonoras.

La definición de datos personales consta de cuatro componentes esenciales que están estrechamente ligados y se complementan entre sí, y juntos determinan si cierta información debe ser considerada como un dato personal, estos componentes son:[5]

1) Toda información.
2) Sobre.
3) Identificada o identificable.
4) Persona física.

QUÉ SON LOS DATOS PERSONALES

La expresión "**toda información**" exige una interpretación amplia desde el punto de vista de su naturaleza, contenido y formato.

En cuanto a *la naturaleza*, el concepto de datos personales incluye información tanto objetiva —por ejemplo, nuestra edad—, como subjetiva —opiniones, apreciaciones y valoraciones—, por lo que no es necesario que determinada información sea verídica o probada para que se considere dato personal. Tan es así que las leyes sobre el particular contemplan la posibilidad de que la información incorrecta sea rectificada.

Respecto al *contenido de la información*, se incluye a todos aquellos datos que proporcionan información sobre nuestra persona, comprende la información relativa a la vida privada, familiar, laboral, económica y social, al igual que la considerada "sensible" por su naturaleza particularmente delicada como el estado de salud, la preferencia sexual o las creencias religiosas.[6]

Desde el punto de vista *del formato*, el concepto de datos personales abarca la información en cualquier modo, sea alfabética, numérica, gráfica, fotográfica o sonora, por citar algunas, y puede estar contenida en cualquier soporte como en papel, en la memoria de un equipo informático, en una cinta de video o en un DVD.

No es necesario que la información esté contenida en una base de datos o en un sistema estructurado para que dicha información sea considerada como un dato personal.

En cuanto al componente "**sobre**" se considera que la información concierne a una persona cuando se refiere a ella. Como ejemplo de esto podemos referirnos a los datos que normalmente se incluyen en el expediente que se crea cuando ingresamos a trabajar en cualquier institución o empresa, y que normalmente está bajo resguardo del área de recursos humanos. Estos datos nos conciernen porque se refieren a nuestra persona, lo mismo podemos decir de los resultados de las pruebas médicas que nos realizan y que se integran a nuestro historial médico.

Así, un dato se refiere a una persona si hace referencia a su identidad, características o comportamiento o si esa información se utiliza para determinar o influir en la manera en que se le trata o se le evalúa.[7]

Por lo que hace al tercer componente "**identificada o identificable**" se considera, de modo general, que una persona física es "identificada"

cuando, dentro de un grupo de personas, se la distingue de todos los demás miembros del grupo. Por lo tanto, la persona física es "identificable" cuando, aunque no se le haya identificado todavía, sea posible hacerlo.

Normalmente, la identificación se da a través de datos concretos que se denominan "**identificadores**" y que tienen una relación privilegiada y muy cercana con una determinada persona, por ejemplo, la apariencia, profesión, cargo que ocupa, el nombre. Estos identificadores constituyen lo que las leyes denominan "datos personales".

En este sentido, una persona puede ser identificada directamente por su nombre y apellidos o, indirectamente, por un número de teléfono, las placas de un coche, el número de pasaporte, la clave única de registro de población, o bien, por una combinación de criterios significativos (edad, domicilio, empleo, etc.) que hagan posible su identificación al estrecharse el grupo al que pertenece.

Un dato se refiere a una persona si hace referencia a su identidad, características o comportamiento, o si esa información se utiliza para determinar o influir en la manera en que se le trata o se le evalúa

Así, el que determinados identificadores se consideren suficientes para lograr la singularización de una persona dependerá del contexto de que se trate. De modo que, un apellido muy común no será suficiente para identificar a una persona dentro del conjunto de población de una demarcación territorial, pero sí lo será para identificarla como alumno dentro de un grupo.

Sobra decir que el identificador más común de una persona es el nombre, dato personal por antonomasia (nombre y apellidos) y, en la práctica, la "persona identificada" implica siempre una referencia a dicho nombre. Sin embargo, hay casos en que, para establecer la identidad habrá que combinar el nombre con otros atributos como fecha de nacimiento, domicilio o fotografía, con el fin de evitar la confusión con otras personas del mismo nombre (homonimias).

En aquellos casos en que los identificadores disponibles no permitan individualizar a una persona, ésta aun puede ser "identificable", ya que esa información vinculada con otros datos permitirá distinguir a esa persona de otras.

En este punto, es importante precisar que, para que una persona sea considerada identificable, se deben tomar en cuenta el conjunto de medios que puedan ser razonablemente utilizados para identificar a

dicha persona. De tal suerte que, la simple e hipotética posibilidad de singularizar a un individuo no es suficiente para considerar a la persona como identificable. Si, teniendo en cuenta estos medios, no existe esa posibilidad o la misma es insignificante, la persona no debe ser considerada como "identificable" y la información no debe catalogarse como "datos personales".

La referencia a "**persona física**", cuarto componente en análisis, significa que la protección proporcionada se aplica a personas físicas, es decir, a seres humanos.

Los datos personales son datos relativos a seres vivos identificados o identificables

La Declaración Universal de los Derechos Humanos se refiere al concepto de persona física en su artículo 6, donde se establece que "*todo ser humano tiene derecho, en todas partes, al reconocimiento de su personalidad jurídica*". Por su parte, el Código Civil para el Distrito Federal, dispone que: "*La capacidad jurídica de las personas físicas se adquiere por el nacimiento y se pierde por la muerte; pero desde el momento en que un individuo es concebido, entra bajo la protección de la ley y se le tiene por nacido para los efectos declarados en el presente Código*".[8]

De tal forma que, los datos personales, son datos relativos a seres vivos identificados o identificables, aunque cabe mencionar que la normativa de protección puede aplicarse, en algunos casos, a datos de personas físicas o morales, lo que dependerá de cada legislación en particular. Ejemplo de ello es la Ley de Protección de Datos Personales del Estado de Colima,[9] la cual establece que los datos de carácter personal son aquellos relativos a personas físicas o morales que de manera directa o indirecta puedan conectarse con una persona específica (artículo 3).[10]

Tema 4. Protección de Datos Personales

La protección de datos personales es un derecho que consiste en ofrecer a los individuos los medios para controlar el uso ajeno de la información personal que les concierne.[11]

Este derecho, también conocido como *habeas data* es, por un lado, un instrumento legal para proteger el derecho a la vida privada y, por otro, una forma de derecho de acceso a la información, que consiste

en que todo individuo tenga garantizado el derecho de acceder a la información que le concierne personalmente.

El origen de este derecho, se vincula al desarrollo de la noción de protección de la privacidad, adquiriendo posteriormente, un perfil conceptual y alcance más diferenciado al punto de convertirse en un derecho autónomo distinto de la intimidad:

La función del derecho fundamental a la protección de datos, es garantizar a toda persona el poder de control sobre sus datos personales, tanto su uso como su destino, con el propósito de impedir su tráfico ilícito y la potencial vulneración de la dignidad del afectado. Esto lleva implícito el poder de disposición sobre sus datos. Por el contrario, la función del derecho a la intimidad, es proteger de cualquier invasión los reductos de vida personal o familiar que la persona desea mantener fuera del saber de terceros, o de evitar intromisiones contra su propia voluntad.[12]

Una definición amplia de este derecho, indica que comprende la prerrogativa que toda persona tiene para:

a) Conocer de su inclusión en bancos de datoso registros.

b) Acceder a toda información que sobre ella conste en los bancos de datos o registros.

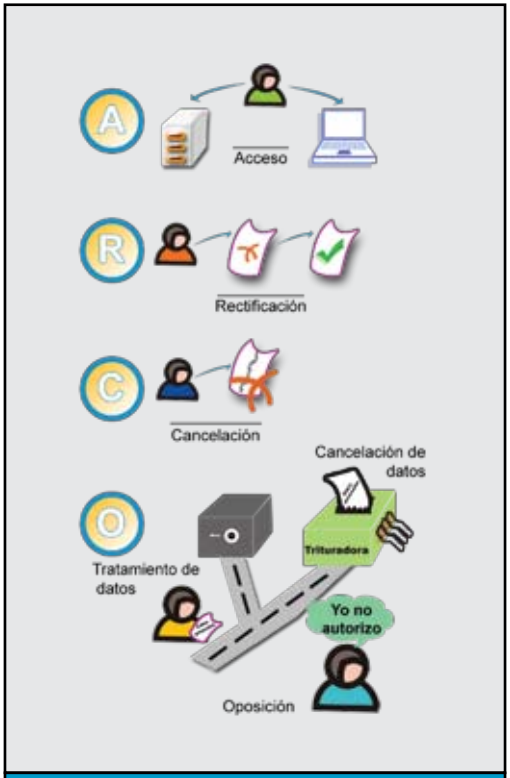
c) Actualizar o corregir, en su caso, la información que sobre ella conste en los bancos de datos o registros.

d) Conocer el propósito o fines para los que se va a utilizar la información que conste sobre ella en los bancos de datos.

e) Que se garantice la confidencialidad de determinada información obtenida legalmente para evitar su conocimiento por terceros.

DATOS PERSONALES

f) Que se garantice la supresión de información sobre la persona con datos sobre su filiación política o gremial, creencias religiosas, vida íntima y toda aquella que pudiera de un modo u otro producir discriminación.[13]



ARCO: Cuatro derechos fundamentales

La protección de datos de carácter personal, es una de las claves esenciales del respeto a la vida privada dentro de la defensa de los derechos humanos y las libertades fundamentales, por ello es importante que las leyes de transparencia y acceso a la información pública, contemplen como excepción al derecho de acceso, el derecho a la vida privada y la intimidad de las personas, a menos que existan intereses colectivos superiores que justifiquen una intromisión en este derecho personalísimo.

El derecho a la protección de datos personales, está integrado por una serie de prerrogativas, principios y procedimientos para el tratamiento de información que concierne a personas físicas, no sólo por parte del Estado o los entes públicos, sino también, por parte de terceros o personas de derecho privado.

Este poder de control sobre los datos personales se manifiesta a través de los denominados derechos ARCO (Acceso, Rectificación, Cancelación y Oposición), a través de los cuales las personas tienen la facultad de:

- ❒ Conocer en todo momento quién dispone de sus datos y para qué están siendo utilizados.
- ❒ Solicitar rectificación de los datos en caso de que resulten incompletos o inexactos.
- ❒ Solicitar la cancelación de los mismos por no ajustarse a las disposiciones aplicables.
- ❒ Oponerse al uso de sus datos si es que los mismos fueron obtenidos sin su consentimiento.

A efecto de garantizar la debida protección de los datos personales, además de establecer los derechos ARCO, las leyes en la materia incluyen una serie de principios rectores en el tratamiento de este tipo de datos como son: el de finalidad, calidad, consentimiento, deber de información, seguridad, confidencialidad, disponibilidad y temporalidad. El incumplimiento de estos principios, constituye una vulneración a la protección de datos personales y, lógicamente, tienen como consecuencia una sanción.

Los principios generales de protección de datos constituyen el contenido esencial del derecho a la protección de datos personales y configuran un sistema de tutela que garantiza un uso racional de los datos personales.

Finalmente, un pilar fundamental para la efectiva protección de datos personales, se encuentra representado por la existencia de órganos garantes que cuenten con un cierto grado de autonomía de gestión e independencia frente a los poderes estatales típicos y ante los cuales, los particulares puedan exigir la tutela de sus derechos relacionados con la protección de datos personales. Para el caso del Distrito Federal, esta labor está encomendada al Instituto de Acceso a la Información Pública del Distrito Federal (InfoDF).

Síntesis

Intimidad es la esfera personal y privada de comportamientos, acciones y expresiones que no deseamos hacer públicos. La intimidad, en una sociedad democrática es uno de los derechos fundamentales necesitados de protección. No sólo porque significa una barrera a la intromisión del Estado sino, también, porque permite el desarrollo íntegro de la personalidad de los ciudadanos.

El derecho a la intimidad se compone de una fase negativa (pasiva) que consiste en el derecho del individuo a vivir en paz y en soledad; y de una fase positiva (activa), constituida por el principio de autodeterminación informativa o de poder de control sobre los datos personales.

La privacidad constituye un conjunto más amplio, más global de facetas de nuestra personalidad que, aisladamente consideradas, pueden carecer de un significado en sí mismo pero que, coherentemente enlazadas entre sí, arrojan un retrato de nuestra personalidad que tenemos derecho a mantener reservada.

Un dato personal, es toda información referida a un individuo que lo identifica o lo hace identificable. Dicha información puede ser numérica, alfabética, gráfica, acústica o de cualquier otro tipo y estar contenida en cualquier soporte.

El derecho a la protección de datos personales consiste en la facultad de los individuos de controlar la información que les concierne y está integrado por una serie de principios y prerrogativas.

Este derecho se compone de los llamados derechos ARCO: acceso, rectificación, cancelación y oposición. Para su tutela es necesaria la existencia de órganos autónomos ante los cuales puedan acudir aquellas personas que consideren que su derecho ha sido violentado. ■

AUTOEVALUACIÓN

Cuestionario sobre los contenidos generales del módulo uno, “Conceptos y Definiciones Básicas”.

1. Tienen derecho a la protección de datos personales:

A. Los entes públicos.
B. Las naciones.
C. Las sociedades anónimas.
D. Los individuos.

2. Es un dato personal:

A. La voz.
B. La huella digital.
C. Número de la licencia de manejo.
D. Todas las anteriores.

3. Para una efectiva garantía del derecho a la protección de datos personales es necesario:

A. La Asamblea Legislativa.
B. La policía.
C. Un órgano autónomo garante.
D. Un escudo.

Antecedentes de las Leyes de Protección de Datos Personales

Módulodos

Temario

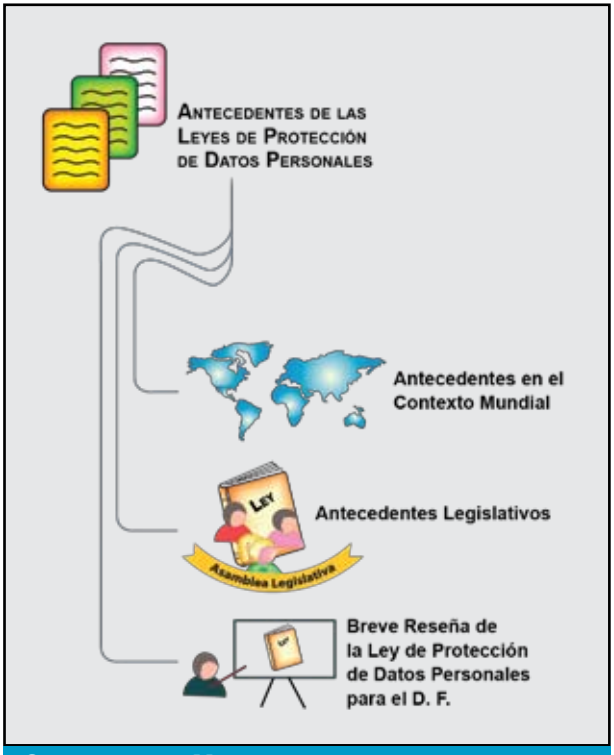
Introducción

Una vez que estudiamos los conceptos básicos relacionados con la protección de datos personales, los cuales son fundamentales para la comprensión de las leyes en la materia, en este módulo abordaremos de manera general, el contexto mundial en el cual fueron creadas las primeras normas en protección de datos personales, así como la institucionalización de este derecho en nuestro país.

Asimismo, se presenta una breve reseña histórica que da cuenta de los hechos más significativos en el proceso de creación y aprobación de la LPDPDF.

El presente módulo abordará los siguientes temas:

1) Antecedentes de las Leyes de Protección de Datos Personales en el Contexto Mundial.
2) Antecedentes Legislativos en Materia de Protección de Datos.
3) Breve Reseña de la Ley de Protección de Datos Personales para el D. F.



Contenido del Módulo Dos

Objetivo del módulo

Al final del módulo los participantes podrán:

- Conocer y explicar de dónde surge el derecho a la protección de datos personales teniendo una idea clara de las causas y el contexto en el que se dieron las primeras leyes en la materia.

Tema 1. Antecedentes de las Leyes de Protección de Datos Personales en el Contexto Mundial

Antes de la aparición de la denominada “revolución tecnológica”, las personas gozaban de una protección natural de carácter operativo y físico frente a intromisiones con respecto a su vida, costumbres, salud, bienes, etcétera. La actividad de investigación estaba reservada a ciertas áreas del Estado y sólo a pocas organizaciones privadas, especialmente las de mayor evolución tecnológica.

A partir de la segunda mitad del siglo XX se empiezan a producir una serie de avances científico-tecnológicos vertiginosos: se perfeccionan las computadoras, se gesta la inteligencia artificial, se inicia el trabajo con el concepto de red y, este perfeccionamiento, sumado a la reducción de costos, permite su masificación a nivel mundial.

En ese momento nace un nuevo paradigma: el de la Sociedad de la Información, en la que la riqueza está basada en la creación intelectual y la capacidad de producir, almacenar y distribuir información, opuesta a la fabricación en serie, la manufactura y las posesiones materiales consideradas como pilar económico de las naciones en la era industrial.

El Internet lanza al mercado de la información una inmensa masa de datos aparentemente inofensivos pero que, cuidadosamente reciclados, tienen capacidad para lesionar derechos de las personas constitucionalmente protegidos, como son la intimidad y la privacidad.[14]

Esta generalización del uso de las tecnologías de la información (TICs), así como el incremento de la utilización de las mismas en las actividades cotidianas del ser humano, han provocado una revolución que impacta los campos social, ideológico, cultural, político y económico.

> Es así que el siglo XXI comienza con un despliegue tecnológico estelar. No puede concebirse más la vida de los seres humanos ni su interacción, sin el uso de tecnologías *urbi et orbi.*[15] Dicha expansión conlleva el intercambio de flujos de información incluida la relativa a las personas. Ahora es posible a través de distintos medios acceder a la información de millones de seres humanos y sus actividades en cualquier parte del planeta. Sin embargo, frente al terreno ganado en materia de libertad de información y expresión, se ha irrumpido silenciosamente en el ámbito de lo privado, ya que la sencilla obtención de cualquier tipo de dato sobre una persona física posibilita la generación de perfiles sobre ella y afectar la esfera de sus derechos y libertades. Por ello puede afirmarse que los horizontes para la privacidad se están transformando en tierra incógnita debido a que sin que el propio titular del dato se entere, terceros —sean entes públicos o privados— tratan su información a través de la utilización de todo tipo de tecnologías como la minería de datos, la geo-localización, la detección remota o la videovigilancia, todo lo anterior conectado a la *world wide web*, tecnologías que hoy en día ya han madurado y están plenamente disponibles en cualquier lugar del mundo.[16]

El Internet lanza al mercado de la información una inmensa masa de datos aparentemente inofensivos pero que, cuidadosamente reciclados, tienen capacidad para lesionar derechos de las personas constitucionalmente protegidos, como son la intimidad y la privacidad

Frente a esta gran problemática generada en materia de protección a la privacidad con la evolución de las tecnologías de la información, diversos organismos y países, desde hace algunas décadas, han detectado la necesidad de regular en materia de protección a la intimidad y privacidad. En este sentido se han creado diversos instrumentos internacionales que aportan a este tema como es el de derechos humanos, así como regulaciones formuladas por bloques económicos como la Unión Europea, la Organización para la Cooperación y el Desarrollo Económico, y del Foro de Cooperación Económica Asia Pacífico, así como la resolución que en esta materia elaboró la Organización de las Naciones Unidas.

Adicionalmente, se han hecho algunos llamamientos, como el de la Cumbre Mundial de la Sociedad de la Información, dirigidos a solicitar a todos los países que garanticen el respeto a la privacidad y a la protección de información y datos personales, ya sea mediante la adopción de legislaciones, la aplicación de marcos de colaboración, mejores prácticas y medidas tecnológicas y de autorregulación por parte de empresas y usuarios.

Tema 2. Antecedentes Legislativos en Materia de Protección de Datos

En Europa, las primeras legislaciones se adoptan en los años setenta, al igual que en los Estados Unidos donde la ley correspondiente se emitió en 1974 con la "*Privacy Act*".

Estas normas son fruto de la inquietud que mostraban las autoridades estatales ante el imparable impulso tecnológico, que tempranamente se manifestó como un peligro potencial para los derechos de los ciudadanos, principalmente, para aquellos derechos más ligados a la personalidad y dignidad de las personas.

Los horizontes para la privacidad se están transformando en tierra incógnita debido a que sin que el propio titular del dato se entere, terceros —sean entes públicos o privados— tratan su información a través de la utilización de todo tipo de tecnologías

Podemos decir que, en los Estados Unidos, se ha adoptado una política mucho más flexible sobre privacidad y protección de datos que en la Unión Europea, cuyo objetivo es proteger y tutelar los derechos de consumidores, la población vulnerable y más aún, se caracteriza por la adopción de un esquema más liberal para el sector empresarial. Han confiado sus políticas de regulación y privacidad a sus empresas porque saben que el gobierno está consciente de que estas acciones y mecanismos fomentan y reactivan el comercio electrónico, no sólo a nivel interno sino también a nivel mundial, promueven las inversiones del sector de las tecnologías de información y sobre todo permiten que las pequeñas y medianas empresas puedan realizar actividades de comercio electrónico en todos los niveles.[17]

También fueron numerosas las respuestas supranacionales que se reflejaron en importantes textos, sin duda, antecedentes de las actuales normas sobre protección de las personas frente al auge informático; así, cabe recordar la Recomendación de la OCDE[18] de 23 de septiembre de 1980 sobre flujo internacional de datos, o las sucesivas Recomendaciones del Parlamento y del Consejo de Europa, que alentaron a los Estados europeos en su desarrollo legislativo frente a la potencial amenaza de las nuevas tecnologías, o los principios o directrices de protección de datos tempranamente aprobados por las Naciones Unidas.

Paulatinamente, la protección de datos como derecho autónomo fue ganando terreno en la concepción general. En el ámbito del Consejo de Europa, se aprobó el Convenio No. 108, del 28 de enero de 1981, para la Protección de las Personas con respecto al Tratamiento

Automatizado de Datos de Carácter Personal, cuyo objetivo (artículo 1º) es el de "garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona" ("protección de datos").

El concepto de vida privada en relación con la protección de datos personales ha sido objeto de interpretación extensiva. En este sentido, el Tribunal Europeo de Derechos Humanos, entiende que también incluye las relaciones personales y las comerciales, citando, precisamente la Convención 108.

Efectivamente, no sólo la intimidad o la vida privada están en juego cuando se trata de protección de datos personales. El principio de calidad de los datos, con sus consecuencias de derecho a la exactitud, actualización, rectificación y supresión, no siempre está directamente vinculado a la privacidad, sino, también cuando se trata de proteger el derecho a la no discriminación o la igualdad de trato en las decisiones individuales automatizadas.[19]

PROTECCIÓN LEGAL ANTE INTERESES COMERCIALES

Ahora bien, en el ámbito comunitario europeo, una norma general que abordara la problemática de la protección de datos personales se hizo esperar hasta el año 1995, y en verdad puede decirse que su aprobación estuvo siempre rodeada de importantes dificultades y que contó en numerosas ocasiones con la resistencia de importantes Estados europeos, que no veían con buenos ojos que una norma comunitaria entrara a regular ámbitos legislativos que en sus derechos nacionales ya habían alcanzado una respuesta satisfactoria, con lo que se entendía que esta nueva norma comunitaria significaría a todas luces una intromisión en sus legislaciones nacionales.

Pese a todas las reservas, en 1995 se aprueba, tras importantes resistencias, la Directiva 95/46/CE, del 24 de octubre sobre protección de datos personales, cuyo objeto y finalidad no se articula sobre la limitación en la actividad informática para asegurar la tutela de los derechos personales, sino sobre la libre circulación de los datos en Estados de acuerdo con la necesaria protección de las personas; esto es, se pretende conciliar la libre circulación de información como instrumento necesario para el progreso de las actividades económicas, políticas y sociales con la necesaria e insalvable tutela de los derechos y libertades de los ciudadanos, pero sin que el recurso a estos derechos pueda constituir nunca por sí sólo una traba u obstáculo al progreso informático.

Después vendrá, al amparo de esta Directiva, la aprobación de normas sectoriales para la protección de datos personales en el ámbito comunitario europeo; así, la Directiva 97/66/CE del 15 de diciembre sobre protección de datos personales y de la intimidad en el sector de las telecomunicaciones, o el Reglamento 45/2001 del 18 de diciembre, para la protección de las personas respecto al tratamiento de datos por instituciones y organismos comunitarios.

La Directiva 95/46/CE constituye el texto de referencia, a escala europea, en materia de protección de datos personales. Crea un marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea (UE). Con ese objeto, la Directiva fija límites estrictos para la recogida y utilización de los datos personales y solicita la creación, en cada Estado miembro, de un organismo nacional independiente encargado de la protección de los mencionados datos.

Tema 3. Breve Reseña de la Ley de Protección de Datos Personales para el D. F.

El propósito de esta reseña es ofrecer un panorama cronológico sobre los eventos más importantes que dieron lugar a la elaboración, aprobación y promulgación de la Ley de Protección de Datos Personales en el Distrito Federal y que dé cuenta del proceso de institucionalización de este derecho.

8 de mayo de 2003: Se publica en la Gaceta Oficial del Distrito Federal (GODF) la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal, la cual dedicaba uno de sus capítulos a la tutela de los datos personales (Capítulo V, del Título Primero).

28 de marzo de 2008: Se publica en la Gaceta Oficial del Distrito Federal (GODF) la nueva Ley de Transparencia y Acceso a la Información Pública del Distrito Federal, la cual abroga[20] a la de 2003 y prevé la obligación de la Asamblea Legislativa de aprobar, en un plazo no mayor a 60 días hábiles, la legislación respectiva a datos personales en el Distrito Federal.

27 de agosto de 2008: La Asamblea Legislativa aprueba el Dictamen presentado por la Comisión de Administración Pública Local por el que se crea la Ley de Protección de Datos Personales para el Distrito Federal.

3 de octubre de 2008: Se publica en la Gaceta Oficial del Distrito Federal el Decreto por el que se expide la Ley de Protección de Datos Personales para el Distrito Federal, la cual entró en vigor al día siguiente de su publicación.

26 de octubre de 2009: Se publican en la Gaceta Oficial del Distrito Federal, los Lineamientos para la Protección de Datos Personales en el Distrito Federal que el Pleno del Instituto de Acceso a la Información Pública del Distrito Federal, aprobó mediante acuerdo 547/SO/14-10/2009.

Garantizar a cualquier persona física, sean cuales fueren su nacionalidad o residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal

Síntesis

El derecho a la protección de datos personales surge ante la evolución tecnológica por el riesgo que representaba la amenaza a los derechos fundamentales, sobre todo a la intimidad y a la privacidad, el manejo indiscriminado de información personal.

Frente a esta gran problemática generada en materia de protección a la privacidad con la evolución de las tecnologías de la información, diversos organismos y países, desde hace algunas décadas, han emitido regulaciones en materia de protección a la intimidad y privacidad.

Se han creado diversos instrumentos internacionales que aportan a este tema como es el de derechos humanos, así como regulaciones formuladas por bloques económicos como la Unión Europea, la Organización para la Cooperación y el Desarrollo Económico, y del Foro de Cooperación Económica Asia Pacífico, así como la resolución que en esta materia elaboró la Organización de las Naciones Unidas.

Las personas contaban con la protección de datos personales en el Distrito Federal desde la aparición de la primera Ley de Transparencia en el año 2003, pero fue hasta 2008 que se contó con una Ley específica sobre el particular. El 26 de octubre 2009, se publican en la Gaceta Oficial del Distrito Federal, los Lineamientos para la Protección de Datos Personales.

Autoevaluación

Cuestionario sobre los contenidos generales del módulo dos, “Antecedentes de las Leyes de Protección de Datos Personales”.

1. Las primeras legislaciones sobre datos personales se adoptan:

A. En los años cuarenta.
B. En los noventa.
C. En los setenta.
D. En el siglo XXI.

2. El texto de referencia para los países europeos para legislar en materia de datos personales es:

A. Privacy Act.
B. Directiva 95/46/CE.
C. Convenio 108.
D. Recomendación de la OCDE del 23 de septiembre de 1980 sobre flujo internacional de datos.

3. La Ley de Protección de Datos Personales para el Distrito Federal data de:

A. 2003.
B. 2005.
C. 1995.
D. 2008.

Aspectos Relevantes de la Ley de Protección de Datos Personales para el Distrito Federal (LPDPDF)

Módulo tres

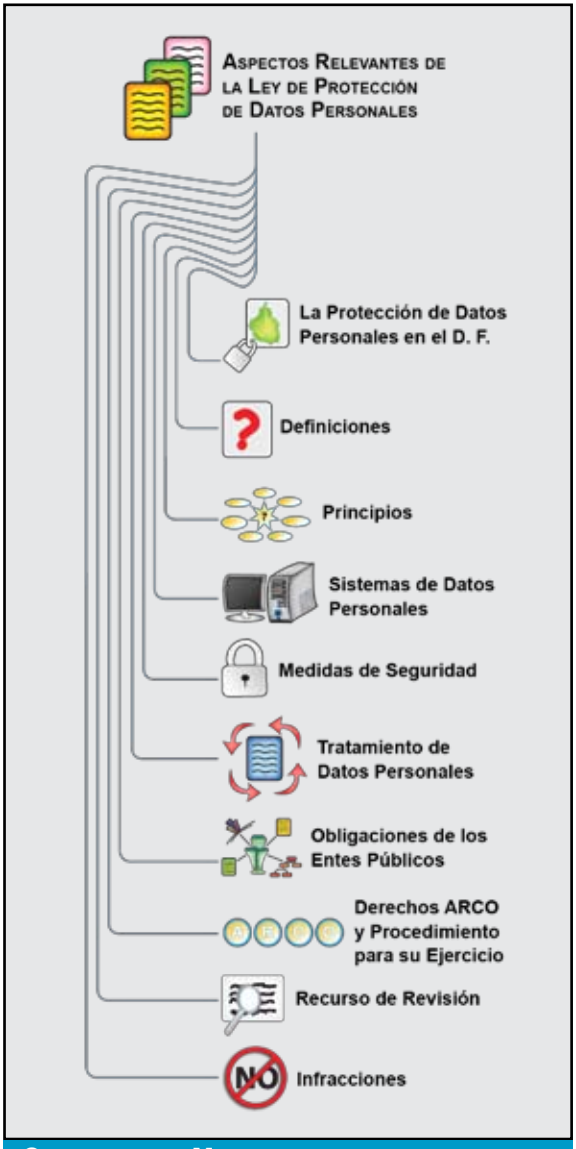
Introducción

En este módulo haremos un recorrido sobre los aspectos establecidos en la LPDPDF, y los Lineamientos de desarrollo de la misma. En ellos se presentan, entre otras cuestiones, definiciones de los términos utilizados y objetivos de la Ley, así como disposiciones generales.

Se clarificarán además algunos de los términos utilizados que son importantes para el mejor entendimiento de la normatividad y se explicarán los principios fundamentales para la interpretación del derecho a la protección de datos personales.

El presente módulo abordará los siguientes temas:

1) La Protección de Datos Personales en el D. F.
2) Definiciones.
3) Principios.
4) Sistemas de Datos Personales.
5) Medidas de Seguridad.
6) Tratamiento de Datos Personales.
7) Obligaciones de los Entes Públicos.
8) Instituto de Acceso a la Información Pública del Distrito Federal.
9) Derechos ARCO y Procedimiento para su Ejercicio.
10) Recurso de Revisión.
11) Infracciones.



Contenido del Módulo tres

Objetivos del módulo

Al final del módulo los participantes podrán:

- ❒ Conocer los aspectos fundamentales que establecen la LPDPDF y los Lineamientos.
- ❒ Comprender los objetivos que persigue la Ley.
- ❒ Familiarizarse con los términos más importantes utilizados en ambas normas.

Tema 1. La Protección de Datos Personales en el D. F.

En la Ley de Protección de Datos Personales para el Distrito Federal (LPDPDF), en vigor desde el 4 de octubre de 2008, no encontramos una definición de "protección de datos personales", sin embargo la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal (LTAIPDF) la define como "*la garantía que tutela la privacidad de datos personales en poder de los entes públicos*".

Cabe señalar que los datos personales en posesión de los entes públicos gozaban de protección legal en el Distrito Federal desde la aparición de la primera Ley de Transparencia en 2003, que dedicaba uno de sus capítulos a la tutela de los datos personales. Sin embargo, con la entrada en vigor de la nueva LTAIPDF, en mayo de 2008, hubo un periodo en el cual las personas se quedaron sin la posibilidad de ejercer los derechos ARCO, pues fue hasta octubre del mismo año, en que recobró vigencia esta posibilidad de protección de datos personales con la publicación de la LPDPDF.

La nueva LTAIPDF excluyó de su regulación a la tutela de los datos personales, así como el capítulo relativo al sistema de archivos, estableciendo en sus artículos transitorios, la obligación de la Asamblea Legislativa de aprobar la legislación respectiva a datos personales y archivos públicos del Distrito Federal.[21]

Los diputados consideraron que era necesario proteger el derecho del titular de los datos personales concentrados en sistemas de información en poder de los entes públicos, de manera que quien posea, administre, utilice o trate de algún modo esos datos, lo haga de tal forma

que no se vulnere el legítimo derecho a la intimidad de las personas y que, además, se defienda la privacidad de los ciudadanos mediante un órgano que controle el cumplimiento de la Ley.

Asimismo, se tomó en consideración la importancia que tiene que las personas tengan a su alcance mecanismos para conocer la información que de ellas obra en los archivos de cualquier ente público, y así poder ejercer los derechos de acceso, rectificación, cancelación y oposición.

Y, con el objeto de brindar seguridad al tratamiento de la información personal, se establecieron una serie de obligaciones que tienen que observar los responsables del manejo de datos personales, así como de toda persona que intervenga en éste.

La Ley y los Lineamientos emitidos por el Instituto de Acceso a la Información Pública del Distrito Federal, para el desarrollo y aplicación de ésta, tienen una estructura muy similar, la diferencia radica en que en los últimos no hay un capítulo de principios, ni de responsabilidades; y, que sólo hay uno relativo a los derechos y el procedimiento para su ejercicio, en tanto que en la Ley son tres, la cual está conformada de la siguiente forma:

TÍTULO PRIMERO:

Disposiciones comunes para los entes públicos.

TÍTULO SEGUNDO:

De la tutela de datos personales.

TÍTULO TERCERO:

De la autoridad responsable del control y vigilancia.

TÍTULO CUARTO:

De los derechos y del procedimiento para su ejercicio.

TÍTULO QUINTO:

De las responsabilidades.

Vale la pena resaltar que, al momento de la aplicación de la normatividad de protección de datos personales, es necesario recurrir, de manera simultánea y paralela a los contenidos, tanto de la Ley, como de los Lineamientos, pues éstos últimos son complementarios a la Ley y, sin ellos, algunos aspectos serían de difícil aplicación.

Los datos personales en posesión de los entes públicos gozaban de protección legal en el Distrito Federal desde la aparición de la primera Ley de Transparencia en 2003

Tema 2. Definiciones

Tanto la LPDPDF, como los Lineamientos que la desarrollan, contienen un apartado de definiciones que nos ayudan a comprender y aplicar las normas pues se precisa lo que se debe entender por los términos que más se utilizan en ellas.

En este sentido, veremos que los términos “bloqueo”, “datos personales”, “responsable”, “sistema de datos personales”, entre otros, son utilizados frecuentemente en el cuerpo de ambas normas. Y, con el fin de no ser repetitivos con el contenido de éstas, sólo mencionaremos que las definiciones están previstas en el artículo 2 de la Ley y en el numeral 3 de los Lineamientos y que, como anexo a este Manual se incluye un glosario de términos que facilitarán el entendimiento del derecho a la protección de datos personales.

Sin embargo, cabe señalar que algunos conceptos que se encuentran definidos en la Ley también lo están en los Lineamientos, pues se consideró conveniente que ciertas definiciones se precisaran con el fin de facilitar la comprensión de los términos, por ejemplo:

Ley	Lineamientos
Bloqueo de datos personales: La identificación y reserva de datos personales con el fin de impedir su tratamiento	Bloqueo: Conservación de datos personales con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo, legal o contractual, de prescripción de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su eliminación del sistema a que correspondan
Responsable del Sistema de Datos Personales: Persona física que decida sobre la protección y tratamiento de datos personales, así como el contenido y finalidad de los mismos	Responsable: El servidor público de la unidad administrativa a la que se encuentre adscrito el sistema de datos personales, designado por el titular del ente público, que decide sobre el tratamiento de datos personales, así como el contenido y finalidad de los sistemas de datos personales

Ley	Lineamientos
Sistema de Datos Personales: Todo conjunto organizado de archivos, registros, ficheros, bases o banco de datos personales de los entes públicos, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso	Sistema de Datos Personales: Conjunto organizado de datos personales que estén en posesión de los entes públicos, contenidos en archivos, registros, ficheros, bases o bancos de datos, que permita el acceso a datos con arreglo a criterios determinados, cualquiera que fuere la modalidad de su creación, almacenamiento, organización o acceso

Como se puede apreciar, en los Lineamientos se detallan con mayor precisión definiciones contenidas en la Ley, con el objeto de otorgar más claridad a términos que son fundamentales para la aplicación de esta normatividad.

Una cuestión relevante es que la LPDPDF establece que la interpretación de la misma debe ser conforme a la Constitución y a los distintos instrumentos internacionales suscritos por México en materia de derechos humanos, así como la interpretación que sobre los mismos hayan realizado los órganos internacionales respectivos.

Esta previsión da atribuciones a los órganos que aplican la Ley, como es el caso del InfoDF, de contar con herramientas interpretativas amplias, pues pueden acudir a los textos de las sentencias dictadas por órganos protectores de derechos humanos en el ámbito internacional, como es el caso de la Comisión y Corte Interamericana de Derechos Humanos.

Y, en la interpretación de esta Ley, será muy importante tener en cuenta que la protección de datos personales cuenta ya con la categoría de ser derecho humano reconocido en la Constitución Federal, por lo que se deberá acudir a la interpretación que sobre las garantías individuales y su fuerza expansiva, ha hecho la Suprema Corte de Justicia de la Nación.

Para cuestiones procedimentales, se prevé que sea de aplicación supletoria la Ley de Procedimiento Administrativo del Distrito Federal (LPADF) y, en su defecto, el Código de Procedimientos Civiles.

Un ejemplo de cuestiones no previstas en la Ley y que, por tanto, requieren de la aplicación supletoria de otra, lo encontramos para en el caso de la representación legal, pues la LPDPDF sólo refiere que el interesado o su representante, pueden presentar una solicitud para ejercer un derecho ARCO, sin que se delimite cómo debe acreditarse tal representación.

Sobre el particular, la LPADF establece que, en el caso de las personas físicas, la representación debe acreditarse mediante instrumento público y, también, mediante carta poder firmada ante dos testigos y ratificadas las firmas ante fedatario público, o bien, por declaración en comparecencia personal ante la autoridad competente (artículo 41).

Tema 3. Principios

Los principios de la protección de datos constituyen el pilar mediante el cual se articula este derecho y son de observancia obligatoria para todo aquél que interviene en el tratamiento de datos personales desde el momento de la obtención hasta la destrucción de los mismos.

Dado su carácter obligatorio, los responsables de los sistemas de datos personales adscritos a los entes públicos, deben adoptar las medidas necesarias para evitar que se produzca una vulneración de los mismos, ya que esto representaría una infracción a la Ley. Es por ello, que es de suma importancia que todo aquel que intervenga en el tratamiento de este tipo de datos, conozca y respete estos principios.

Principios de la protección de datos

Principios que incorpora la LPDPDF (artículo 5):

- ❒ Licitud.
- ❒ Consentimiento.
- ❒ Calidad de los datos.
- ❒ Confidencialidad.
- ❒ Seguridad.
- ❒ Disponibilidad.
- ❒ Temporalidad.[22]

Principio de licitud, se refiere a que los entes públicos sólo deben desarrollar o tener sistemas de datos personales que estén relacionados directamente con las facultades y atribuciones que les han sido asignadas. Es por ello, que tanto los datos que obtienen, como la posesión y el tratamiento de los sistemas de datos personales, deben obedecer únicamente a las atribuciones legales o reglamentarias de cada ente público.

Los sistemas de datos personales, no pueden tener finalidades contrarias a las leyes o la moralidad pública y en ningún caso pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.

En este sentido, la posesión de sistemas que no estén directamente vinculados con las atribuciones de un ente público violenta este principio. Sin embargo, el tratamiento posterior de datos con fines históricos, estadísticos o científicos no se considera incompatible.

Ejemplo:

> Los datos de un padrón de beneficiarios de un programa para adultos mayores pueden ser utilizados para enviar información a los interesados sobre la apertura de un nuevo centro de atención en su localidad (finalidad compatible). Sin embargo, no podrán usarse para pedir el voto (finalidad incompatible).

En definitiva, los datos personales no pueden ser tratados para fines distintos a los que motivaron su obtención, pues esto supondría una vulneración al principio de licitud, así como un nuevo uso de los datos que requeriría del consentimiento del interesado para su tratamiento.

Si sucediera el caso de que, por alguna causa, la finalidad del tratamiento cambie, los datos deberán ser cancelados, ya que su uso para finalidades distintas a las informadas al interesado, como ya lo hemos mencionado, no está permitido, salvo que sea para fines históricos, estadísticos o científicos.

Los principios de la protección de datos constituyen el pilar mediante el cual se articula este derecho

Principio de consentimiento, constituye uno de los principios básicos sobre los que se articulan la mayor parte de las legislaciones de protección de datos de carácter personal. Se refiere a la *voluntad libre, inequívoca, específica e informada*, mediante la cual el interesado accede a que sus datos personales sean tratados.

En los Lineamientos se detalla lo que debemos entender por:

a) *Libre*: Cuando es obtenido sin la intervención de vicio alguno del consentimiento.

b) *Inequívoco*: Cuando existe expresamente una acción que implique la existencia del consentimiento.

c) *Específico*: Cuando se otorga referido a una determinada finalidad.

d) *Informado*: Cuando se otorga con conocimiento de las finalidades para las que el mismo se produce.

En este sentido, el consentimiento debe ser obtenido libre de coacción y basado en información veraz y clara, asimismo, debe ser comprobable. La doctrina señala que este principio es el eje fundamental a partir del cual se construye el derecho a la protección de datos personales y que conlleva la idea de la *autodeterminación informativa*.[23]

Los datos personales no pueden ser tratados para fines distintos a los que motivaron su obtención

En suma, el consentimiento implica que todo tratamiento de datos requiere de nuestra autorización previa. Sin embargo, debemos considerar también que las leyes y, en particular, la LPDPDF, contemplan un catálogo amplio de excepciones en las cuales no es necesario el consentimiento para que nuestros datos personales sean tratados (artículo 16).

Principio de calidad, se refiere a que los datos obtenidos deben ser *ciertos, adecuados, pertinentes y no excesivos* en relación al ámbito y finalidad para los que fueron recabados, de forma tal que éstos deben responder con veracidad a nuestra situación actual. Esto quiere decir que los datos no sólo tienen que estar actualizados sino que deben ser adecuados y útiles respecto a las finalidades para las cuales nos fueron solicitados.

Entenderemos por:

a) *Cierto*: Cuando los datos se mantienen actualizados de tal manera que no se altere la veracidad de la información, ya que esto podría traer como consecuencia que el titular se vea afectado por esta situación.

b) *Adecuado*: Cuando se observa una relación proporcional entre los datos recabados y la finalidad del tratamiento.

c) *Pertinente*: Cuando es realizado por el personal autorizado para el cumplimiento de las atribuciones de los entes públicos que los hayan recabado.

d) *No excesivo*: Cuando la información solicitada al titular de los datos es la estrictamente necesaria para cumplir con los fines para los cuales se hubieran recabado.

El principio de calidad implica entonces que los datos deberán mantenerse constantemente actualizados. Ello no supone que el responsable tenga que investigar activamente para proceder a la actualización, sino solamente realizar la actualización cuando tenga la posibilidad de conocer que un dato se encuentra desactualizado o que es inexacto.

Otro medio de actualización de los datos es el que realiza el propio interesado mediante el ejercicio del derecho de rectificación, previsto en el artículo 28 de la LPDPDF.

Los datos de carácter personal pueden estar almacenados en el sistema correspondiente en diferentes estados: activos y cancelados

Ejemplo:

> En un programa social que va a otorgar un apoyo a jóvenes para terminar sus estudios de bachillerato, no se debe solicitar el dato de si la persona está afectada por una minusvalía, ya que ese dato no es relevante para otorgar la ayuda.

Debemos tener en cuenta que, cuando los datos ya no resultan necesarios, o no se ajusten a la finalidad para la que fueron recabados, deberán ser eliminados del sistema correspondiente (**principio de temporalidad**). De igual forma los datos podrán cancelarse en cualquier momento cuando exista la solicitud de ejercicio de derecho de cancelación por parte del interesado. En este caso, pudiera darse la situación de que exista una obligación legal que imponga conservar los datos, éstos, en vez de ser eliminados del sistema, deberán ser bloqueados, es decir, se deberá suspender el tratamiento de los datos, dejándolos como en una especie de congeladora, de forma que sólo resulten accesibles a las autoridades competentes durante el periodo que señale la obligación legal de que se trate.

En este sentido, el Código Financiero del Distrito Federal, establece la obligación de conservar la documentación y demás elementos contables y comprobatorios durante un periodo de 5 años, el cual sería aplicable, por ejemplo, al padrón de Impuesto sobre Nóminas.

Por tanto, los datos de carácter personal pueden estar almacenados en el sistema correspondiente en diferentes estados: activos, lo que supone que pueden ser tratados mientras son necesarios para cumplir la finalidad para la cual fueron obtenidos y cancelados cuando ya no son necesarios para dicha finalidad.

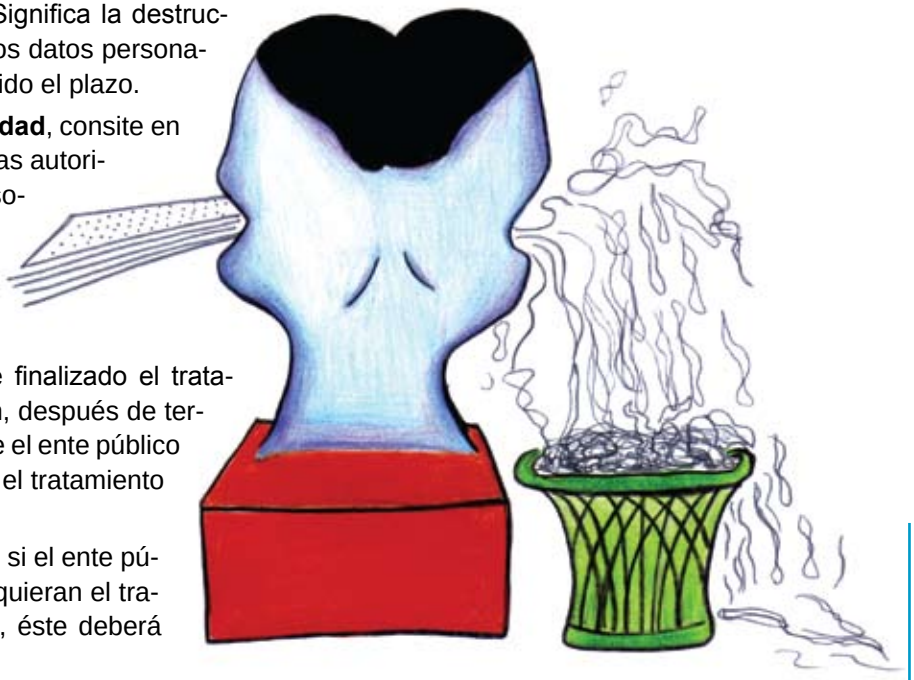
A su vez, los datos cancelados pueden encontrarse en dos situaciones distintas:

Boqueados. Los datos sólo están disponibles para la tramitación de posibles responsabilidades derivadas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades.

Eliminación de los datos. Significa la destrucción o desaparición física de los datos personales bloqueados una vez cumplido el plazo.

Principio de confidencialidad, consite en garantizar que sólo las personas autorizadas accedan a los datos personales para su tratamiento con la obligación de observar el deber de secrecía.

El deber de confidencialidad subsiste aun después de finalizado el tratamiento de los datos y, también, después de terminada la relación laboral entre el ente público y las personas que realizaban el tratamiento de datos personales.



ELIMINAR DATOS INNECESARIOS O SIN FINALIDAD JURÍDICA

Este principio conlleva que, si el ente público contrata servicios que requieran el tratamiento de datos personales, éste deberá asegurarse de que, en los instrumentos jurídicos que correspondan a esa contratación, se estipule la obligación de garantizar la seguridad y confidencialidad de los sistemas de datos personales, así como la prohibición de utilizarlos con propósitos distintos a los establecidos en el contrato, mismo que deberá contemplar penas convencionales en caso de incumplimiento.

Ejemplo de cláusula de confidencialidad:

> Las partes asumen la obligación de guardar secreto profesional sobre cuanta información pudieran recibir, gestionar y articular con relación a los datos personales y a no comunicarlos a terceros, salvo excepciones legales, así como a

destruirlos, cancelarlos o devolverlos en el momento de la finalización de la relación contractual entre ambas partes, así como a aplicar las medidas de seguridad necesarias.

Principio de seguridad, este consiste en garantizar que únicamente el responsable del sistema de datos personales o en su caso las personas debidamente autorizadas puedan llevar a cabo el tratamiento de los datos personales mediante procedimientos establecidos para este efecto.

En este sentido, el responsable deberá adoptar las medidas de índole técnica y organizativa que sean necesarias a fin de garantizar la integridad, confiabilidad, confidencialidad y disponibilidad de los datos de carácter personal y así evitar su alteración, pérdida, tratamiento o acceso no autorizado.

Para ello la ley prevé la existencia de un documento de seguridad, el cual, desde el punto de vista de la seguridad de la información, tiene el carácter de documento interno de una organización y constituye un pilar fundamental de las políticas de seguridad ya que tiene como objetivo principal recoger todas las medidas, normas, procedimientos, reglas y estándares de índole técnica y organizativa que permitan garantizar los niveles de seguridad en el tratamiento de los datos personales.

Desde el punto de vista jurídico, el cumplimiento de las medidas técnicas y organizativas dispuestas en el documento de seguridad, tiene como finalidad garantizar el derecho de protección de datos de carácter personal de los sistemas que almacena y trata el ente público para el cumplimiento de sus atribuciones legales.

El **documento de seguridad** debe contener como mínimo:

- ❒ El ámbito de aplicación.
- ❒ Las medidas, normas, procedimientos de actuación, reglas y estándares utilizados.
- ❒ Las funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal.

- ❒ La estructura de los sistemas de datos personales que contengan datos de carácter personal y la descripción de los sistemas de información que los tratan.
- ❒ El procedimiento de notificación, gestión y respuesta ante incidencias.
- ❒ Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.
- ❒ Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.

La legislación en materia de protección de datos, establece que el documento de seguridad deberá mantenerse actualizado y ser revisado siempre que se produzcan cambios relevantes en los sistemas de información o en el tratamiento de datos de la empresa o entidad.

Principio de disponibilidad, se refiere a que los datos deben almacenarse de forma tal que se nos permita, en todo momento, el ejercicio de los derechos de acceso, rectificación, cancelación y oposición. Los sistemas de datos personales, deben organizarse de tal manera que el acceso a los datos personales contenidos en él sea ágil.

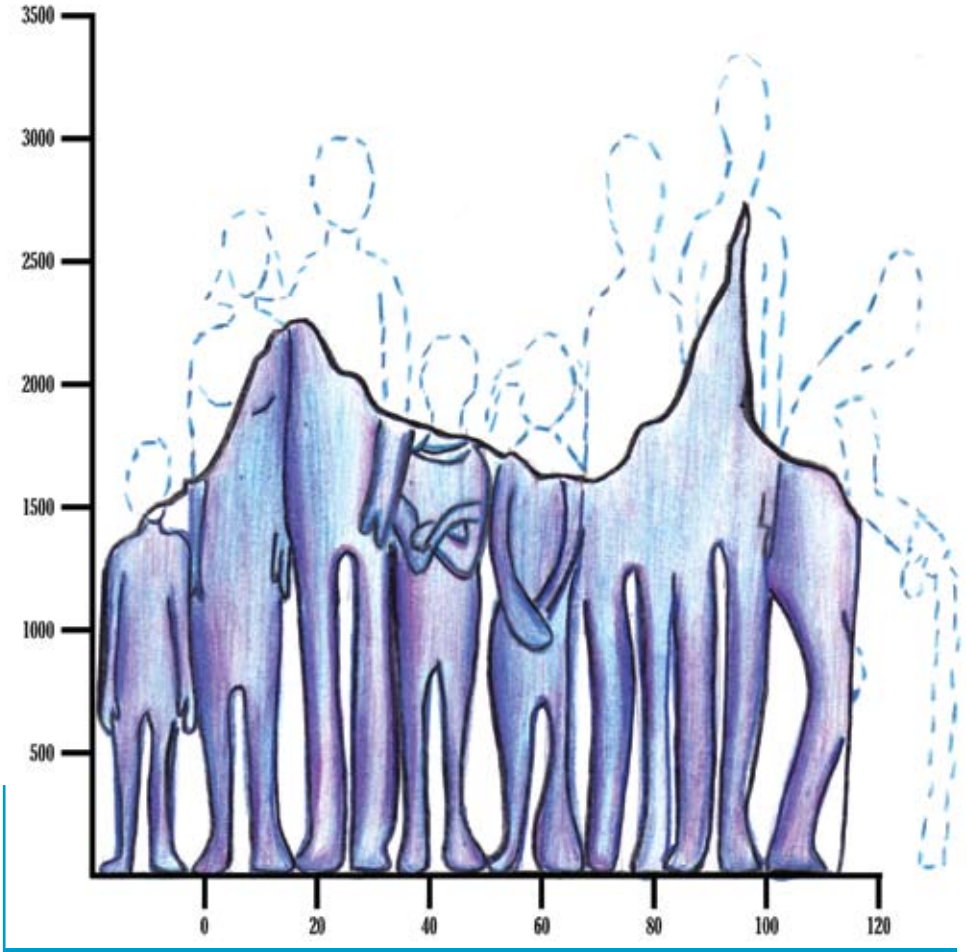
Así, bajo una organización adecuada, se facilita que, ante solicitudes de derechos ARCO, se nos pueda dar una pronta respuesta, ya que los datos sobre los cuales ejercemos estos derechos estarán disponibles para una respuesta en tiempo y forma a nuestra solicitud.

Principio de temporalidad, según este principio, los datos personales deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los que fueron obtenidos. También se denomina principio de caducidad, e implica la conservación limitada de los datos, es decir, éstos sólo deben mantenerse mientras sean necesarios para el cumplimiento de la finalidad que motivó su recolección.

Cabe señalar que no se violentaría este principio, si los datos son tratados posteriormente para fines estadísticos o científicos, siempre y cuando, sean previamente disociados.[24]

Por tanto, los datos se conservarán en una forma que permita la identificación de los interesados durante un periodo no superior al necesario para el cumplimiento de los fines para los que fueron obtenidos o para los que se traten posteriormente.

La Ley prevé también que los datos pueden ser conservados de manera íntegra y permanente, únicamente, para fines históricos.



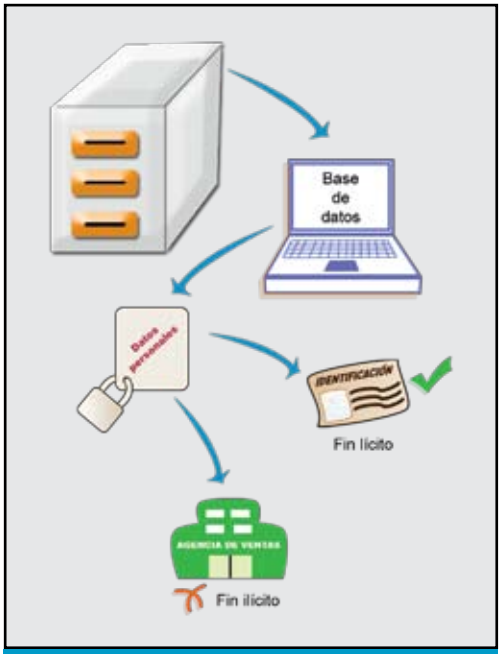
Tema 4. Sistemas de Datos Personales[25]

De acuerdo con lo que establece la Ley, un sistema de datos personales consiste en todo conjunto organizado de archivos, registros, ficheros, bases o banco de datos personales de los entes públicos, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso.

La cuestión a dilucidar es cómo identificar si estamos en presencia de un sistema de datos personales o no y, por tanto, si hay obligación de cumplir con las disposiciones que la LPDPDF determina. En la práctica, la identificación de estos sistemas no es una labor sencilla, ya que la definición legal no ayuda a delimitar su contenido.

Sin embargo, algunos factores que pueden resultar útiles para determinar si estamos ante un sistema de datos personales son la finalidad, los usos previstos, las personas de las que se obtendrán los datos, la descripción de éstos y el órgano responsable del sistema.

Así, estaremos en presencia de un sistema de datos personales si estamos ante un conjunto de datos que se obtienen de un colectivo de personas para el cumplimiento de una finalidad determinada. Esta finalidad, comúnmente, está estrechamente vinculada al ejercicio de competencias legales y al cumplimiento de funciones administrativas. Entonces, serán las funciones y atribuciones normativas que requieren se recabe información personal de los ciudadanos, las que darán lugar a la identificación de un sistema de datos personales.



Cómo funciona el sistema

Por ello, la identificación de los sistemas de datos personales existentes en un ente determinado, debe realizarse a partir de las competencias administrativas, atribuciones normativas o funciones, que justifican el desarrollo de una actividad y la existencia de procesos de gestión pública donde se manejan datos personales.[26]

Un sistema de datos personales se identifica, entonces, por el propósito o finalidad con la que se tratan los datos de carácter personal

contenidos en éste, sobre el cual deberán cumplirse las obligaciones contenidas en la Ley y demás normativa aplicable, tales como su registro ante el InfoDF y la adopción de las medidas de seguridad que correspondan según la categoría de datos que los sistemas incluyan.

Al interior de un sujeto obligado por la Ley encontraremos, al menos, sistemas de datos personales relativos al personal que labora en el ente y sistemas de proveedores y, dependiendo de su actividad específica, habrá sistemas de beneficiarios, contribuyentes, becarios, prestadores de servicio social y otros sistemas específicos que obedecerán a la especialidad de las atribuciones que tiene cada institución.

Es importante que los sistemas de datos personales en posesión de los entes públicos, se inscriban en el registro que al efecto habilite el InfoDF

A la vista de estos ejemplos, en los sistemas de personal se incluyen datos de los empleados que son necesarios para el inicio y mantenimiento de la relación laboral, tales como nombre, domicilio, Registro Federal de Contribuyentes (RFC), así como trayectoria académica y profesional. Datos similares se pueden encontrar en los sistemas de proveedores, como son nombre o razón social, RFC, datos bancarios para transferencias como la CLABE (Clave Bancaria Estandarizada) necesarios para el desarrollo de la adquisición de bienes o servicios.

Entonces, un sistema de datos personales, es un conjunto organizado de datos de carácter personal, cualquiera que sea su soporte, organización o acceso, siempre que tenga una estructura que permita un fácil acceso a los datos de una persona determinada.

Por otro lado, los sistemas deben responder a un nivel de desglose semejante al de la actividad que los entes desarrollan. En este sentido, si existe una delimitación de sus diferentes atribuciones se debe, por ende, poder especificar las distintas finalidades de los sistemas de datos personales.

Por ejemplo, si un mismo ente presta diversos servicios sociales, tales como atención médica a domicilio, ayuda económica, uniformes escolares gratuitos, apoyo a madres solteras, lo lógico es que tenga un sistema de datos personales para cada uno de estos servicios, ya que prestar uno u otro implica la obtención de datos distintos en cada uno de los supuestos.

Por disposición legal,[27] a cada ente público le corresponde determinar a través de su titular o, en su caso del órgano competente, la

creación, modificación y supresión de sistemas de datos personales de acuerdo a su ámbito de competencia. Así, en el caso de la Jefatura de Gobierno, correspondería a su titular, el Jefe de Gobierno, esta determinación. En el caso del InfoDF, correspondería al Pleno, al ser éste la instancia directiva, en tanto que dicha facultad, en el caso del Instituto Electoral del Distrito Federal, está atribuida al Consejo General. Esto dependerá de la estructura de cada ente.

ASPECTOS DE TODO SISTEMA DE DATOS PERSONALES

Esta determinación debe ser publicada en la Gaceta Oficial del Distrito Federal y es necesario incluir, en los casos de creación de sistemas de datos personales, al menos, los siguientes aspectos:

a) La finalidad del sistema de datos personales y los usos previstos para el mismo.

b) Las personas o grupos de personas sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.

c) El procedimiento de recolección de los datos de carácter personal.

d) La estructura básica del sistema de datos personales y la descripción de los tipos de datos incluidos en el mismo.

e) De la cesión de las que pueden ser objeto los datos.

f) Las instancias responsables del tratamiento del sistema de datos personales.

g) La unidad administrativa ante la que podrán ejercitarse los derechos de acceso, rectificación, cancelación u oposición.

h) El nivel de protección exigible.

En caso de que el titular decida cambiar el sistema de datos personales en cualquiera de los anteriores aspectos, dicha modificación también debe publicarse en la Gaceta Oficial indicando cuáles de éstos fueron modificados.

Las disposiciones que se dicten para la supresión de sistemas de datos personales, deben indicar el destino que vaya a darse a los datos contenidos en los mismos o, en su caso, las medidas previstas para su destrucción. En este caso, podrán excluirse aquellos datos que, previa disociación, sean tratados para finalidades estadísticas o históricas.

Un sistema de datos personales es un conjunto organizado de datos de carácter personal, cualquiera que sea su soporte, organización o acceso, siempre que tenga una estructura que permita un fácil acceso a los datos de una persona determinada

La publicación en la Gaceta Oficial del Distrito Federal, de los acuerdos por medio de los cuales se determina la creación de un sistema de datos personales, además de darle publicidad al acto, permite dotar a dichos acuerdos de cierta fuerza normativa, ya que con ello, los interesados cuentan con certeza jurídica acerca de la finalidad del tratamiento que van a recibir los datos que proporcionen y, de la instancia a la que pueden acudir a ejercer los derechos que la Ley les otorga.

Es importante que los sistemas de datos personales en posesión de los entes públicos, se inscriban en el registro que al efecto habilite el InfoDF, ya que esto permitirá a los interesados, conocer los sistemas de datos personales que obran en las distintas dependencias locales, y les facilitará, también, el ejercicio de sus derechos ARCO.

La información que debe contener el registro es similar a la del acuerdo de creación de un sistema de datos personales. Los Lineamientos regulan con mayor detalle, los campos que deben contener tanto el acuerdo de creación como los del registro:

Creación	Registro
I. Denominación del sistema de datos personales, indicando normativa aplicable, así como la descripción de la finalidad y usos previstos	I. Nombre del Sistema y, en su caso, fecha de publicación en la Gaceta Oficial del Distrito Federal
II. El origen de los datos, indicando el colectivo de personas sobre las que se pretende obtener datos de carácter personal, o que resulten obligados a suministrarlos; su procedencia (propio interesado, representante, ente público, etcétera) así como el procedimiento de obtención de los mismos (formulario, Internet, transmisión electrónica, etcétera)	II. Nombre y cargo del responsable del sistema
III. La estructura básica del sistema con descripción detallada de datos identificativos y, en su caso, de los especialmente protegidos, así como las restantes categorías de datos de carácter personal; modo de tratamiento utilizado en su organización (manual o automatizado). En su caso, señalar los datos de carácter obligatorio y facultativo	III. Identificación del sistema, finalidades y usos previstos, así como el soporte en el que se encuentra
IV. Las cesiones de datos que se tengan previstas, indicando, en su caso, los destinatarios o categorías de destinatarios	IV. La categoría de los datos personales contenidos en el sistema, forma de recolección y actualización de los mismos
V. La identificación de la unidad administrativa a la que corresponde el sistema de datos personales, así como del cargo del responsable	V. Unidad administrativa en la que se encuentra el sistema
VI. Domicilio oficial y dirección electrónica de la Oficina de Información Pública	VI. Destino y personas físicas o morales a las que puedan ser transmitidos
VII. Indicación del nivel de seguridad que resulte aplicable: básico, medio o alto	VII. Modo de interrelacionar la información contenida en el sistema y el plazo de conservación de los datos

(Continúa en la siguiente página)

(Viene de la página anterior)

Creación	Registro
	VIII. Teléfono y correo electrónico del responsable
	IX. Normativa aplicable al sistema
	X. Indicación del nivel de seguridad aplicable: básico, medio o alto

Un principio fundamental que se regula en el capítulo en estudio, es la obligación de cumplir con el denominado "**deber de información**" o "derecho de información al interesado", el cual constituye el fundamento previo necesario para el correcto funcionamiento de un esquema jurídico de protección de datos, ya que sería difícil que se puedan ejercer derechos tales como el de acceso o de oposición al tratamiento de sus datos, si previamente no conocemos en qué sistema y bajo qué parámetros serán tratados nuestros datos.

Los entes públicos tienen deber de informar a los interesados, al momento de recabar datos personales de éstos, de forma expresa, precisa e inequívoca lo siguiente (artículo 9):

1) De la existencia de un sistema de datos personales, del tratamiento de datos personales, de la finalidad de la obtención de éstos y de los destinatarios de la información.
2) Del carácter obligatorio o facultativo de responder a las preguntas que les sean planteadas.
3) De las consecuencias de la obtención de los datos personales, de la negativa a suministrarlos o de la inexactitud de los mismos.
4) De la posibilidad para que estos datos sean difundidos, en cuyo caso deberá constar el consentimiento expreso del interesado, salvo cuando se trate de datos personales que por disposición de una Ley sean considerados públicos.
5) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

6) Del nombre del responsable del sistema de datos personales y en su caso de los destinatarios.

Para el cumplimiento de esta obligación, el InfoDF emitió un acuerdo por medio del cual aprobó la leyenda que deben utilizar los entes públicos para informar a los interesados de estas advertencias:

> **Los datos personales recabados serán protegidos, incorporados y tratados en el Sistema de Datos Personales** (nombre del sistema de datos personales), **el cual tiene su fundamento en** (fundamento legal que faculta al Ente público para recabar los datos personales), **cuya finalidad es** (describir la finalidad del sistema) **y podrán ser transmitidos a** (destinatario y finalidad de la transmisión), **además de otras transmisiones previstas en la Ley de Protección de Datos Personales para el Distrito Federal.**
>
> **Los datos marcados con un asterisco (*) son obligatorios y sin ellos no podrá acceder al servicio o completar el trámite** (indicar el servicio o trámite de que se trate).
>
> **Asimismo, se le informa que sus datos no podrán ser difundidos sin su consentimiento expreso, salvo las excepciones previstas en la Ley.**
>
> **El responsable del Sistema de datos personales es** (nombre del responsable), **y la dirección donde podrá ejercer los derechos de acceso, rectificación, cancelación y oposición, así como la revocación del consentimiento es** (indicar el domicilio de la Oficina de Información Pública correspondiente)**.**
>
> **El interesado podrá dirigirse al Instituto de Acceso a la Información Pública del Distrito Federal, donde recibirá asesoría sobre los derechos que tutela la Ley de Protección de Datos Personales para el Distrito Federal al teléfono: 5636-4636; correo electrónico: datos.personales@infodf.org.mx o www.infodf.org.mx.**

Otro principio básico en materia de protección de datos es el relativo a los datos especialmente protegidos, conocidos como datos sensibles

En los casos en que los datos no fueron obtenidos directamente del interesado, el ente público debe hacer de su conocimiento los aspectos que conforman el deber de información dentro de un plazo de tres meses.

En este sentido, no hay obligación de hacerlo, si el interesado fue informado con anterioridad que:

- ❒ Sus datos están incorporados en un sistema.
- ❒ Del tratamiento.
- ❒ La finalidad y destinatarios de la información.
- ❒ De una posible difusión, en la que habrá que otorgar su consentimiento expreso, salvo que por ley sean considerados públicos.
- ❒ De la posibilidad de ejercer los derechos ARCO.

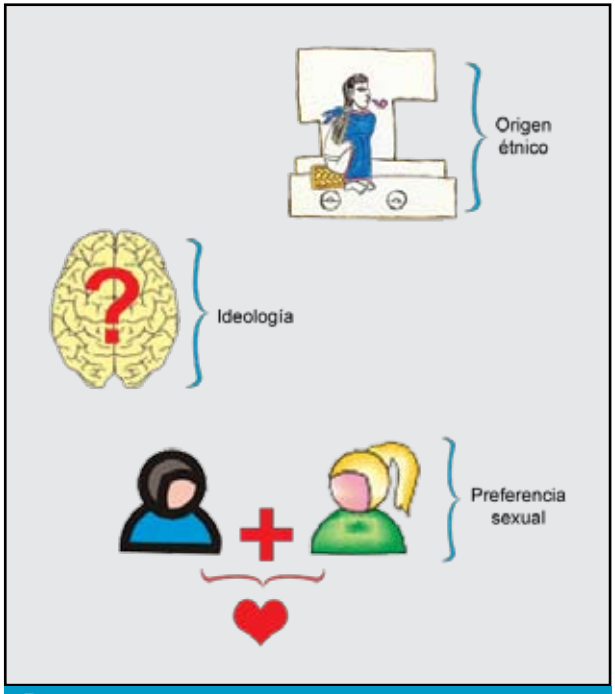
Entonces las excepciones al deber de informar son:

1) Que se haya informado al interesado con anterioridad.
2) Que así lo prevea expresamente una Ley.
3) Cuando los datos provengan de fuentes accesibles al público en general.
4) Cuando resulte imposible o exija un esfuerzo desproporcionado realizar tal comunicación, siempre atendiendo al número de interesados y antigüedad de los datos.

Los datos personales recabados con fines policiales se cancelarán cuando dejen de ser necesarios para las investigaciones que motivaron su almacenamiento

Otro principio básico en materia de protección de datos es el relativo a los **datos especialmente protegidos**, conocidos como datos sensibles. Este es un principio muy importante que establece que nadie está obligado a proporcionar datos como:

- ❒ Origen étnico o racial.
- ❒ Características morales o emocionales.
- ❒ Ideología y opiniones políticas.
- ❒ Creencias.
- ❒ Convicciones religiosas.
- ❒ Ideas filosóficas.
- ❒ Preferencia sexual.



DATOS NO OBLIGATORIOS

En este sentido, está prohibida la creación de sistemas de datos personales que tengan la finalidad exclusiva de almacenar este tipo de datos personales, con la excepción de que sólo pueden ser tratados cuando:

- ❒ Medien razones de interés general.
- ❒ Así lo disponga una ley.
- ❒ Lo consienta expresamente el interesado.
- ❒ Con fines estadísticos o históricos, esto siempre y cuando se hubiera realizado previamente el procedimiento de disociación.

El procedimiento de disociación no es necesario en caso de estudios científicos o de salud pública.

Los **datos sensibles** son aquellos que por su propia naturaleza impulsan a la persona a la más absoluta reserva de dicha información y suponen que su divulgación, le coloque en una situación de vulnerabilidad en el entorno social o familiar. La salud, la sexualidad, la ideología política, así como las creencias religiosas son consideradas como datos sensibles que se colocan en la esfera íntima del ser humano y que sólo el titular del dato puede divulgar.

La protección de datos personales sensibles, tiene como objetivo dificultar la identificación de personas por sus características íntimas que las hacen más vulnerables, se trata, en definitiva, de una protección que se basa en el riesgo de discriminación o de persecución política, social, racial o religiosa.

Los entes públicos están obligados a adoptar medidas de seguridad tan sólo por el hecho de contar con sistemas de datos personales y realizar tratamientos de datos, tanto de particulares, como de servidores públicos

Además de lo relativo a los datos sensibles, en este capítulo, se hace referencia a los sistemas creados con fines administrativos por instituciones de seguridad pública, estableciéndose que los mismos quedarán sujetos al régimen general de protección de la Ley.

Datos de carácter personal obtenidos para fines policiales. Se establece (artículo 11) que pueden ser recabados sin consentimiento y que deben estar limitados a los supuestos y categorías que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la prevención o persecución de los delitos. La obtención y tratamiento de estos datos, solo podrá realizarse en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa, o de la obligación de resolver las pretensiones formuladas por los interesados ante los órganos jurisdiccionales.

Los datos personales recabados con fines policiales se cancelarán cuando dejen de ser necesarios para las investigaciones que motivaron su almacenamiento, y deberán tomarse en consideración aspectos como:

- ❒ La edad del interesado.
- ❒ El carácter de los datos.
- ❒ La necesidad de mantenerlos hasta la conclusión de una investigación o procedimiento concreto.

- ❒ La resolución judicial firme, en especial la absolutoria.
- ❒ El indulto.
- ❒ La rehabilitación.
- ❒ La prescripción de responsabilidad.

Lo que se busca con la cancelación de este tipo de datos, es lo que se conoce como “derecho al olvido” mediante la eliminación de datos caducos. Bajo este principio, determinados datos deben ser borrados de los sistemas transcurrido cierto tiempo desde que sucedió el hecho para el cual se recabaron, esto con la finalidad de evitar que las personas queden prisioneras de su pasado.

En este sentido, si una persona fue parte de una investigación policial pero al final de la misma resultó inocente, tiene derecho a solicitar que sus datos sean eliminados de los archivos policiales y así mantener su reputación intacta.

Los responsables de los sistemas de datos personales con fines policiales, para la prevención de conductas delictivas o en materia tributaria, podrán negar el acceso, rectificación, oposición y cancelación de datos personales, en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o, las necesidades de las investigaciones que se estén realizando, así como cuando los mismos obstaculicen la actuación de la autoridad durante el cumplimiento de sus atribuciones.

Tema 5. Medidas de Seguridad

Los entes públicos están obligados a adoptar medidas de seguridad tan sólo por el hecho de contar con sistemas de datos personales y realizar tratamientos de datos, tanto de particulares, como de servidores públicos.

Las medidas de seguridad previstas en la Ley[28] revisten dos características principales:

1) Se trata de medidas que constituyen mínimos exigibles, por lo que el ente público deberá observarlas sin perjuicio del estado

la tecnología, la naturaleza de los datos almacenados y los riesgos a los que están expuestos. El ente público debe adoptar las medidas adicionales que estime necesarias para garantizar la protección y resguardo de la información.

2) Las medidas son acumulativas, es decir, el nivel medio implica la adopción de medidas de seguridad descritas en este nivel, más las dispuestas para el nivel básico. Las de nivel alto, implican la adopción de las medidas definidas para los tres niveles (básico, medio y alto).

La Ley establece (artículo 13) una serie de obligaciones que deben ser observadas por los entes públicos en cuanto a las medidas de seguridad, mismas que deberán:

1) Responder al nivel de protección que ameriten los datos.
2) Constar por escrito y **comunicar el nivel aplicable al Instituto para su registro**.
3) Señalar nombre y cargo del servidor público responsable del sistema de datos personales.
4) Especificar a la persona física o moral que intervenga como usuario e indicar datos del acto jurídico por el que se otorgó el tratamiento.
5) Notificar al Instituto la actualización de estos datos dentro de los 30 días hábiles siguientes a su modificación.

Se regulan también los tipos y niveles de seguridad que deben adoptarse (artículo 14). La Ley distingue a los tipos de seguridad en:

- ❒ Física.
- ❒ Lógica.
- ❒ De desarrollo y aplicaciones.
- ❒ De cifrado.
- ❒ De comunicaciones y redes.

Por otro lado, se distingue entre medidas de seguridad de nivel básico, medio y alto.

Básico. Se aplica a todos los sistemas de datos personales como:

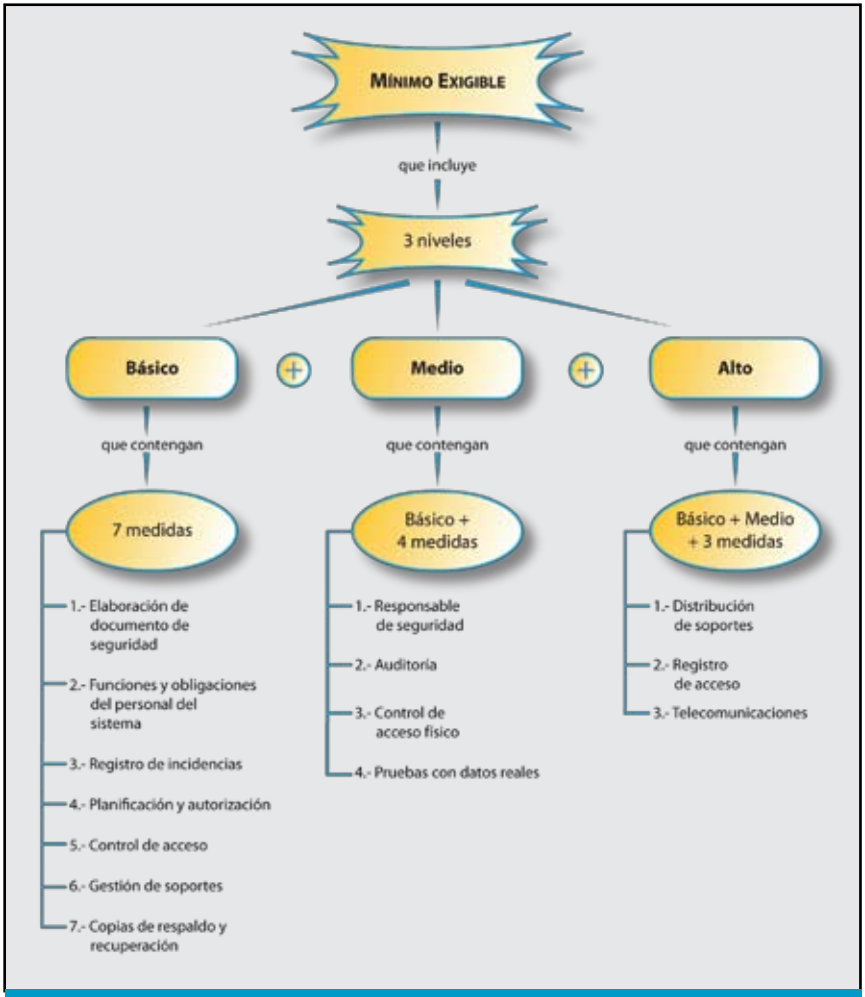
a) Documentos de seguridad.
b) Funciones y obligaciones del personal que intervenga en el tratamiento de los sistemas de datos personales.
c) Registro de incidencias.
d) Identificación y autentificación.
e) Control de acceso.
f) Gestión de soportes.
g) Copias de respaldo y recuperación.

Medio. Aplica a los sistemas que contienen datos relativos a la comisión de infracciones administrativas o penales, hacienda pública, servicios financieros, datos patrimoniales, así como a los sistemas que contengan datos que permitan obtener una evaluación de la personalidad del individuo. Además de las medidas del nivel básico considera los siguientes aspectos:

a) Responsable de seguridad.
b) Auditoría.
c) Control de acceso físico.
d) Pruebas con datos reales.

Alto. Se aplica a sistemas de datos concernientes a ideología, religión, creencias, afiliación política, origen racial o étnico, salud, biométricos, genéticos o vida sexual, así como los que contengan datos recabados para fines policiales, de seguridad, prevención, investigación y persecución de delitos. Los sistemas de datos a los que corresponde adoptar este nivel de seguridad, además de incorporar las medidas de nivel básico y medio, deberán contemplar:

a) Distribución de soportes.
b) Registro de acceso.
c) Telecomunicaciones.



Niveles de seguridad

En los Lineamientos se define al **documento de seguridad**, como el instrumento que establece las medidas y procedimientos administrativos, físicos y técnicos de seguridad aplicables a los sistemas de datos personales, necesarios para garantizar la protección, confidencialidad, integridad y disponibilidad de los datos contenidos en dichos sistemas.

Este instrumento debe generarse para todos los sistemas de datos personales que existan en los entes públicos, ya que es un aspecto de seguridad aplicable a todos los niveles y su contenido variará dependiendo del nivel de cada sistema, por lo que una cuestión fundamental es identificar el tipo de datos contenidos en ellos.

Veamos en qué consisten cada uno de los aspectos correspondientes a los diferentes niveles de seguridad.

Nivel básico, contempla:

La elaboración del **documento de seguridad**, que debe contener:

1) Nombre del sistema.
2) Cargo y adscripción del responsable.
3) Ámbito de aplicación.
4) Estructura y descripción del sistema de datos personales.
5) Especificación detallada de la categoría de datos personales contenidos en el sistema.
6) Funciones y obligaciones del personal que intervenga en el tratamiento de los sistemas de datos personales.
7) Medidas, normas, procedimientos y criterios enfocados a garantizar el nivel de seguridad exigido por la Ley y los presentes Lineamientos.
8) Procedimientos de notificación, gestión y respuesta ante incidencias.
9) Procedimientos para la realización de copias de respaldo y recuperación de los datos.
10) Procedimientos para la realización de auditorías, en su caso.

La responsabilidad de la elaboración del documento de seguridad recae en el responsable del sistema de datos personales

La responsabilidad de la elaboración del documento de seguridad, recae en el responsable del sistema de datos personales y, como ya se ha mencionado, es posible la adopción de medidas adicionales a las establecidas en la Ley, que pueden ser plasmadas en este documento. Su actualización debe realizarse anualmente, o cada vez que se produzcan cambios relevantes en el tratamiento que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas.

Funciones y obligaciones del personal que interviene en el tratamiento de los sistemas de datos personales, deben estar claramente definidas en el documento de seguridad. El responsable, debe adoptar las medidas necesarias para que el personal conozca las normas de seguridad que afecten el desarrollo de sus funciones, así como las responsabilidades y consecuencias en que pudiera incurrir en caso de incumplimiento.

En este punto, es útil apoyarse en el Manual de Organización de la institución, pues se trata de plasmar la clasificación de los puestos de trabajo partiendo de un análisis funcional de la organización, detallar las funciones y obligaciones de los diferentes puestos y especificar las autorizaciones al personal para el tratamiento de datos personales.

Se deben prever, para traslado de la documentación, medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte

Registro de incidencias. Consiste en un procedimiento de notificación y gestión de cualquier anomalía que afecte o pudiera afectar la seguridad de los datos. Este registro, debe plasmarse en una bitácora y contener:

a) La descripción del tipo de incidencia.
b) El momento en que se presentó.
c) Persona que realiza la notificación.
d) A quién se comunica.
e) Los efectos que se hubieran derivado de la misma y las acciones implementadas.

Identificación y autenticación. El primero, consiste en el procedimiento para el reconocimiento de la identidad de la persona que acceda al sistema de datos personales, en tanto que el segundo, se refiere al procedimiento de comprobación de identidad de la persona autorizada para el tratamiento de datos personales. Se aplica a los sistemas de datos personales automatizados, pues se trata de procedimientos de asignación de claves tanto de identificación como de autenticación, en suma, se trata de las claves de usuario y contraseña.

En este sentido, el responsable tiene a su cargo la elaboración de una relación actualizada de los servidores públicos que tienen acceso autorizado al sistema de datos personales, y de establecer procedimientos:

1) Que permitan la correcta identificación y autenticación para el acceso.
2) Que permitan la identificación, de forma inequívoca y personalizada, de toda aquella persona que intente acceder al sistema de datos personales y la verificación de que está autorizada.

Cuando el mecanismo de autenticación se base en la existencia de contraseñas, debe establecerse un procedimiento específico para la asignación, distribución y almacenamiento de las mismas que garantice su confidencialidad e integridad.

Las contraseñas deben ser creadas bajo un procedimiento que especifique su longitud, formato y contenido. La modificación de las mismas, debe realizarse de manera periódica, registrarse en el documento de seguridad y conservarse cifradas.

Control de acceso. Se refiere a los procedimientos que deben existir para regular el acceso a los lugares donde se encuentren instalados o resguardados los sistemas de datos personales.

El responsable debe mantener actualizada la relación de personas y los accesos autorizados para cada una de ellas y solamente él podrá conceder, alterar o anular la autorización para el acceso a los sistemas de datos personales.

Gestión de soportes. Se refiere a que los soportes y documentos que contengan datos de carácter personal permitan identificar el tipo de información que contienen, ser inventariados y ser accesibles sólo por el personal autorizado para ello en el documento de seguridad.

La salida de estos soportes y documentos de los locales bajo el control del responsable, debe ser autorizada por éste, o encontrarse acreditada en el documento de seguridad.

Se deben prever, para traslado de la documentación, medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal, su destrucción o borrado, deberá contemplar medidas encaminadas a impedir el acceso a la información contenida en el mismo o su recuperación posterior.

Copias de respaldo y recuperación. Es el último aspecto que debe incorporarse a las medidas de seguridad del nivel básico y hace alusión a los procedimientos para:

a) La realización de copias de respaldo y su periodicidad. En caso de que los datos personales se encuentren en soporte físico, debe procurarse que el respaldo se efectúe mediante la digitalización de los documentos.

b) Procedimientos para la recuperación de datos de modo que se garantice su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida involuntaria o destrucción accidental.

El periodo de conservación de los datos consignados en el registro de acceso debe ser de, al menos, dos años

El responsable debe verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos. Se trata de que existan procedimientos de recuperación de los datos, de forma que si ocurre algún accidente, se puedan reconstruir y llegar al estado en que estaban al momento de ocurrir el accidente.

Nivel medio de seguridad. Además de las medidas del básico, los aspectos que debe contener son:

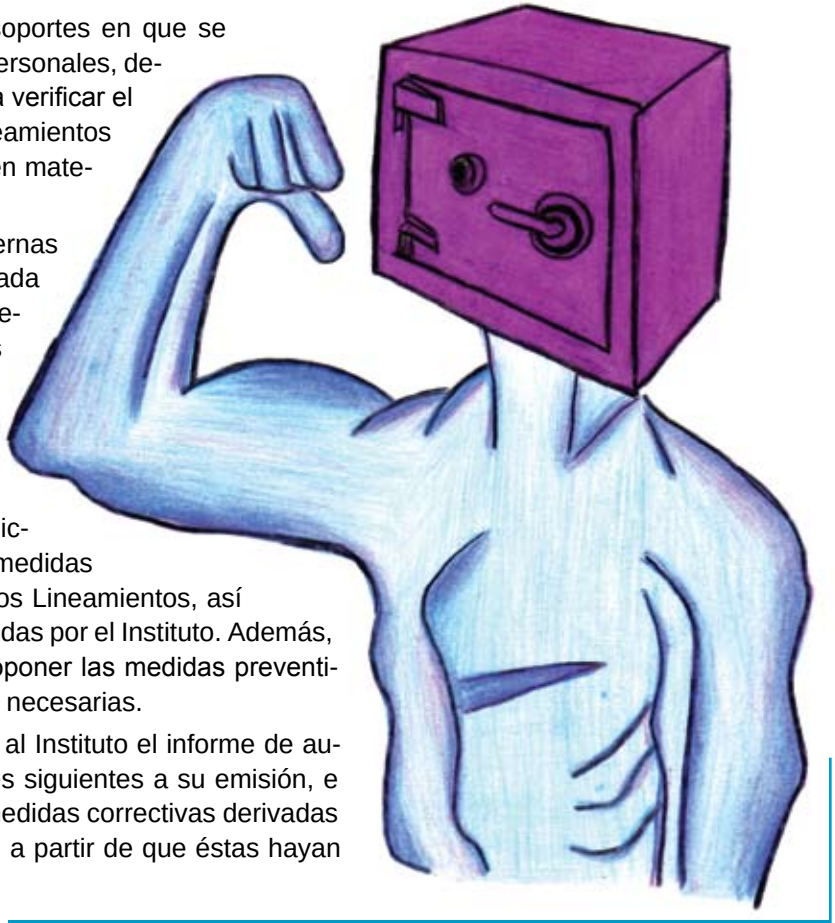
Responsable de seguridad. Persona a la que el responsable del sistema de datos personales asigna formalmente la función de coordinar y controlar las medidas de seguridad aplicables. Debe estar dotado de la autoridad suficiente para implantar y vigilar el cumplimiento de las medidas de seguridad por parte del resto de las personas que intervienen en el tratamiento de datos de un sistema.

Puede haber uno o varios responsables de seguridad para coordinar y controlar las medidas definidas en el documento de seguridad.

La designación puede ser única para todos los sistemas de datos en posesión del ente público, o diferenciada, dependiendo de los métodos de organización y tratamiento de los mismos. Esta designación nunca supone una delegación de las facultades y atribuciones que corresponden al responsable del sistema de datos personales.

En relación con los sistemas automatizados, la figura del responsable de seguridad, se asocia con un perfil técnico, sin embargo, dado que muchas de las medidas de seguridad son organizativas éste no es un requerimiento indispensable.

Auditoría. Las instalaciones y soportes en que se encuentren los sistemas de datos personales, deben ser sometidos a auditorías para verificar el cumplimiento de la Ley, de los Lineamientos y demás procedimientos vigentes en materia de seguridad de datos.



Las auditorías pueden ser internas o externas y deberán efectuarse cada dos años. Las auditorías internas pueden ser realizadas por los órganos de control de los entes públicos, en tanto que las externas por despachos o profesionistas debidamente acreditados.

El informe de resultados, debe dictaminar sobre la adecuación de las medidas de seguridad previstas en la Ley, los Lineamientos, así como en las recomendaciones emitidas por el Instituto. Además, de identificar sus deficiencias y proponer las medidas preventivas, correctivas o complementarias necesarias.

El responsable debe comunicar al Instituto el informe de auditoría dentro de los 20 días hábiles siguientes a su emisión, e informar sobre la adopción de las medidas correctivas derivadas de la auditoría en el plazo referido, a partir de que éstas hayan sido atendidas.

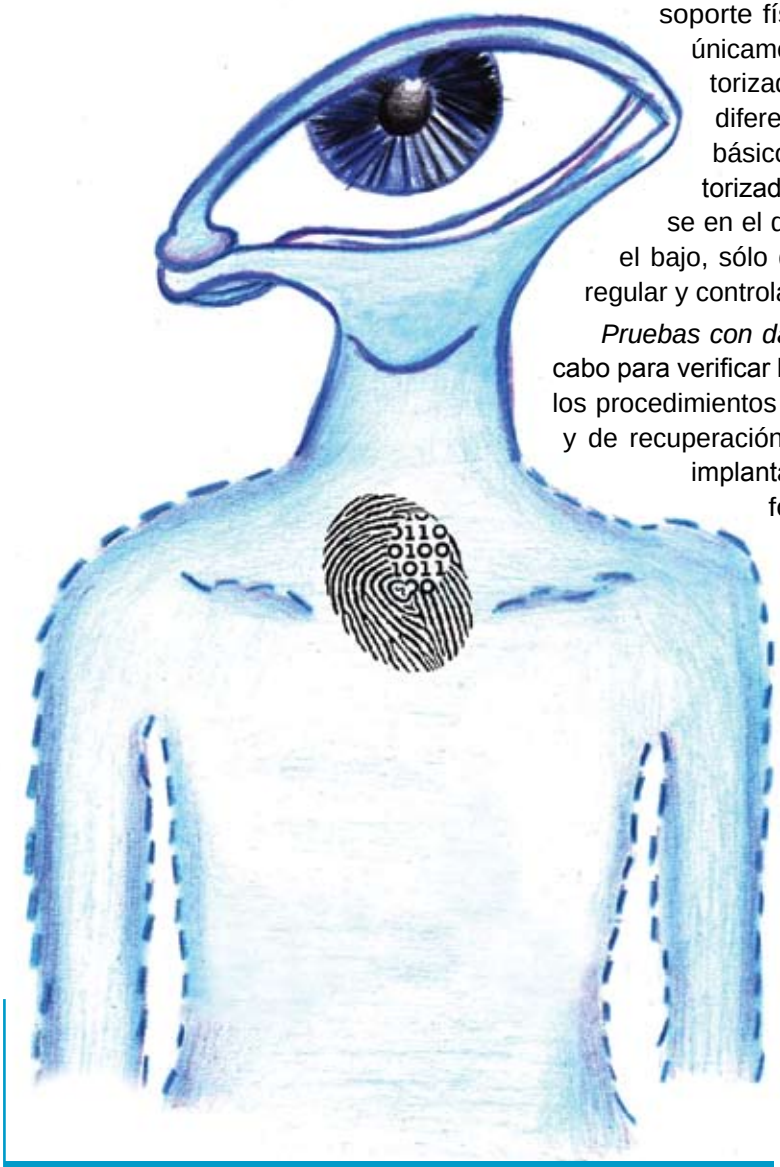
Control de acceso físico. El acceso a las instalaciones donde se encuentren los sistemas de datos personales, ya sea en soporte físico o automatizado, deberá permitirse únicamente a quienes estén expresamente autorizados en el documento de seguridad. La diferencia entre el control de acceso del nivel básico y medio, estriba en que las personas autorizadas en el nivel medio, deberán especificarse en el documento de seguridad, en tanto que en el bajo, sólo deben establecerse procedimientos para regular y controlar el acceso.

Pruebas con datos reales. Las pruebas que se lleven a cabo para verificar la correcta aplicación y funcionamiento de los procedimientos para la obtención de copias de respaldo y de recuperación de los datos, que sean anteriores a la implantación o modificación de los sistemas informáticos que traten sistemas de datos personales, no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de datos tratados.

En caso de que las pruebas se realicen con datos reales, deberá elaborarse una copia de respaldo con anterioridad a fin de evitar su pérdida o alteración durante la realización de las pruebas.

Nivel de seguridad alto. Además de las medidas del básico y medio le corresponde:

Distribución de soportes. La distribución de los soportes que contengan datos de carácter personal, debe realizarse cifrando los datos o utilizando cualquier otro mecanismo que garantice



que dicha información no sea inteligible, ni manipulada durante su traslado o transmisión.

La finalidad última de esta medida es evitar que, ante cualquier incidencia que pueda producirse en la distribución de los datos, o en el soporte que los contiene, personas no autorizadas puedan acceder a la información y modificarla. Por ello, se recomienda la utilización de mecanismos de seguridad mediante claves de acceso a los sistemas, o la encriptación de los datos con programas especializados para evitarlo.

Registro de acceso. Implica que el acceso a los sistemas de datos personales, está limitado exclusivamente al personal autorizado. En el caso en que los sistemas puedan ser utilizados por múltiples autorizados deben existir mecanismos que permitan identificar sus accesos.

Los mecanismos de registro de accesos, estarán bajo el control directo del responsable de seguridad correspondiente, y no estará permitida la desactivación o manipulación de los mismos. De cada acceso deben conservarse como mínimo:

a) La identificación de quien accedió.
b) La fecha y hora.
c) El sistema accedido.
d) El tipo de acceso y si éste fue autorizado o denegado.

El periodo de conservación de los datos consignados en el registro de acceso debe ser de, al menos, dos años.

Todas las aplicaciones o programas internos que traten con datos de carácter personal, deben configurarse para que registren y almacenen los datos de todas aquellas personas que acceden o intentan acceder a la aplicación.

Esta medida de seguridad se ve aumentada en el nivel alto para los sistemas automatizados respecto del registro de accesos: identificación, hora, fichero, tipo de acceso, autorizado o denegado. No es necesario este registro si el responsable del sistema es una persona física y es el único que accede al mismo.

Telecomunicaciones. La transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones

electrónicas, debe realizarse cifrando dichos datos, o bien, utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulable por terceros.

Por lo general, se utilizan redes de telecomunicaciones abiertas para transmitir datos y archivos. Para evitar que durante la transmisión de estos datos puedan producirse intercepciones o manipulaciones no deseadas, deben utilizarse mecanismos de cifrado de los datos con programas especializados, o transmitir datos a través de redes privadas, que garanticen que la comunicación entre dos puntos es segura, y no pueda ser interceptada por terceras personas.

Tema 6. Tratamiento de Datos Personales

Los entes públicos realizan tratamiento de datos personales necesarios para el ejercicio de sus atribuciones, derivado de este tratamiento, deben atender una serie de obligaciones que reflejan la observancia de los principios básicos de la protección de datos, entre ellas:

- ❒ Informar al interesado con carácter previo al tratamiento de los datos de carácter personal.
- ❒ Recabar sólo datos imprescindibles para ejercer sus atribuciones.
- ❒ Facilitar a las personas el ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO).

La Ley, en el capítulo relativo al tratamiento de datos personales, establece que éste requerirá el consentimiento inequívoco, expreso y por escrito del interesado (artículo 16).

El consentimiento del interesado implica, la manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual éste consiente el tratamiento de sus datos personales. Sin embargo, la ley prevé una serie de excepciones a este principio, en las cuales ***no se requiere*** del consentimiento para el tratamiento de datos personales:

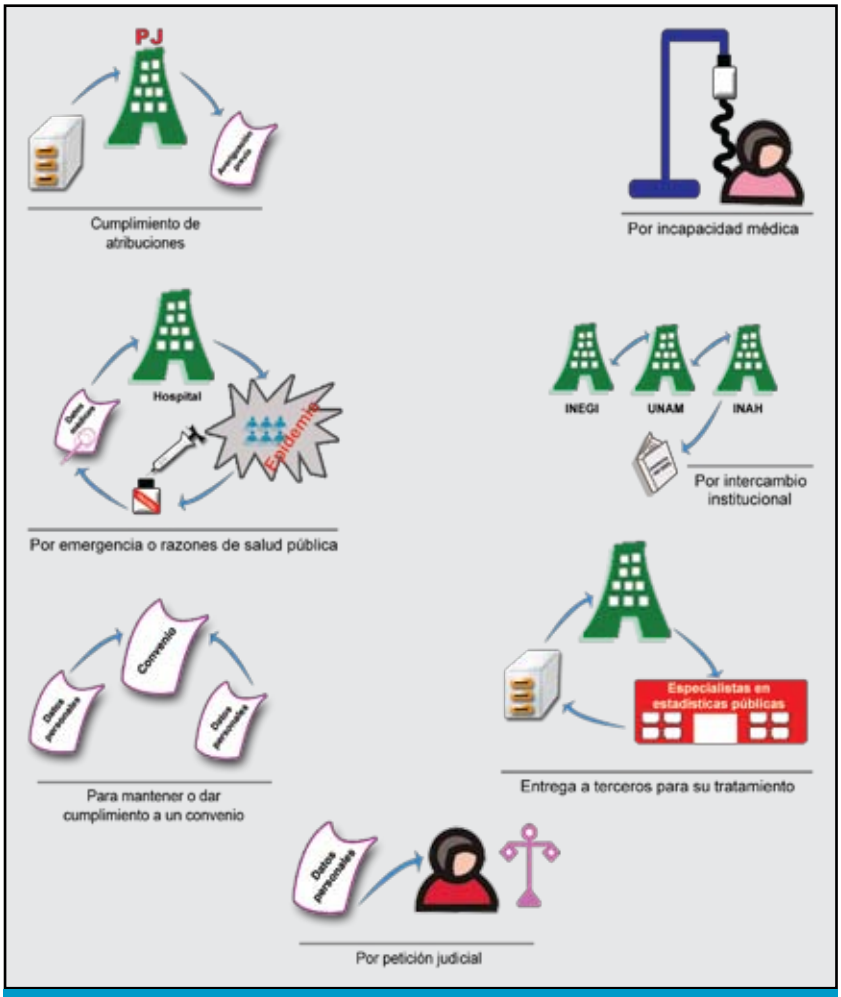
1) En el ejercicio de las atribuciones legales conferidas a los entes públicos. Por ejemplo, cuando la Secretaría de Finanzas solicita datos personales para el ejercicio de su función recaudadora.

2) Cuando los datos se refieren a las partes de un convenio de una relación de negocios, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento. Por ejemplo, no es necesario que se preste el consentimiento cuando los datos personales son utilizados para elaborar una tarjeta para el control de horario, puesto que es deber de los trabajadores cumplir con la jornada laboral y los datos son necesarios para dicho control.

3) Cuando el interesado no está en posibilidad de otorgar su consentimiento por motivos de salud, y el tratamiento de datos es necesario para la prevención o diagnóstico médico, siempre que dicho tratamiento se realice por una persona sujeta al secreto profesional.

4) En materia de salud, si median razones de salubridad pública, de emergencia o para la realización de estudios epidemiológicos, por ejemplo, para la prevención de una eventual epidemia.

5) Cuando la transmisión de datos se encuentre prevista en una ley, como puede ser el acceso a la información contenida en el padrón electoral y en las listas nominales de electores, por parte de los partidos políticos y que está bajo



Cuándo no se requiere consentimiento

resguardo del Instituto Federal Electoral. El acceso a esta información, se encuentra previsto en el Código Federal de Instituciones y Procedimientos Electorales (COFIPE), norma con rango de ley expedida por el Congreso de la Unión.

6) Cuando hay transmisión de datos entre organismos gubernamentales para su tratamiento posterior con fines estadísticos, históricos o científicos. En este sentido, no se requerirá del consentimiento para la transmisión a la información amparada por la Ley del Sistema Nacional de Información Estadística y Geográfica. Esta Ley establece en su artículo 46:

> Las Unidades estarán obligadas a respetar la confidencialidad y reserva de los datos que para fines estadísticos proporcionen los Informantes del Sistema. Los servidores públicos de la Federación, de las entidades federativas y de los municipios, tendrán la obligación de proporcionar la información básica que hubieren obtenido en el ejercicio de sus funciones y sirva para generar Información de Interés Nacional, que les solicite el Instituto en los términos de la presente Ley. Lo anterior, con excepción de los secretos bancario, fiduciario y bursátil, no será violatorio de la confidencialidad o reserva que se establezca en otras disposiciones.

7) La cesión de datos personales de un ente público a la compañía aseguradora con quien tiene contratada la póliza de gastos médicos mayores para sus empleados, no requiere del consentimiento de los interesados, ya que está amparada por la excepción que prevé la cesión de datos a terceros para la prestación de un servicio, siempre y cuando, el tratamiento se limite a una finalidad legítima establecida en un contrato.
8) Cuando media una orden judicial, si una autoridad jurisdiccional requiere acceso a ciertos datos para el desarrollo de su labor, no se considera que se vulnere este principio.
9) Cuando los datos figuren en registros públicos en general y el tratamiento sea necesario, siempre que no se vulneren sus derechos y libertades. En la definición de fuente de acceso público contenida en los lineamientos, se dice que tienen este carácter: los registros públicos, los diarios, gacetas y boletines gubernamentales, así como otros medios oficiales de difusión. Por lo

tanto, la consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, sin más exigencia que, en su caso, el pago de una contraprestación, para acceder a determinado medio de información.

En cuanto al consentimiento, la Ley prevé que éste puede ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos. Por su parte, los Lineamientos precisan que, el interesado podrá revocar su consentimiento mediante solicitud presentada ante la Oficina de Información Pública que corresponda, a través de los formatos que para tal efecto emita el Instituto.

Los interesados deben especificar la finalidad para la cual se revoca el consentimiento para tratar sus datos personales, además de cumplir con los requisitos establecidos en el artículo 34 de la Ley:

1) Nombre del ente público a quien se dirija.
2) Nombre completo del interesado, en su caso, el de su representante legal.
3) Descripción clara y precisa de los datos personales respecto de los que se pretende revocar el consentimiento.
4) Cualquier otro elemento que facilite su localización.
5) El domicilio, mismo que se debe encontrar dentro del Distrito Federal, o medio electrónico para recibir notificaciones.
6) Opcionalmente, la modalidad en la que prefiere se otorgue el acceso a sus datos personales, la cual podrá ser consulta directa, copias simples o certificadas.

El interesado podrá revocar su consentimiento mediante solicitud presentada ante la Oficina de Información Pública que corresponda, a través de los formatos que para tal efecto emita el Instituto

La Oficina de Información Pública realizará las gestiones necesarias ante el responsable que corresponda hasta la culminación del procedimiento conforme al artículo 32 de la Ley, relativo a la recepción y trámite de las solicitudes para ejercer los derechos ARCO.

En caso de que sea procedente la solicitud de revocación del consentimiento, el responsable debe cesar en el tratamiento de los datos, sin perjuicio de la obligación de bloquear los datos conforme a la Ley y Lineamientos.

En el supuesto de que los datos hubieren sido cedidos previamente, el responsable, una vez revocado el consentimiento, deberá comunicarlo a los cesionarios. También se prevé que ante la improcedencia de la revocación del consentimiento, el interesado podrá ejercer su derecho de cancelación.

La revocación del consentimiento sigue el mismo trámite que el utilizado en un supuesto de cancelación, procediéndose al bloqueo de los datos y, posteriormente, al cumplirse el plazo de prescripción de las posibles responsabilidades, a la eliminación de los datos del sistema correspondiente.

Por otra parte, la Ley prevé, en el capítulo sobre tratamiento, que en los supuestos de utilización o cesión de de los datos de carácter personal en que se impida gravemente o se atente de igual modo contra el ejercicio de derechos de las personas, el Instituto podrá requerir a los responsables de los sistemas de datos personales, la suspensión en la utilización o cesión de los datos. Si el requerimiento fuera desatendido, mediante resolución fundada y motivada, el Instituto podrá bloquear tales sistemas, de conformidad con el procedimiento que al efecto se establezca. El incumplimiento a la inmovilización ordenada por el Instituto será sancionado por la autoridad competente de conformidad por la Ley Federal de Responsabilidades de los Servidores Públicos.

La inmovilización a que se refiere el párrafo anterior y que se encuentra prevista en el artículo 17 de la Ley, consiste en una medida cautelar que puede adoptarse en supuestos constitutivos de tratamiento ilícito de datos personales y siempre que el responsable hubiera desatendido el requerimiento previo de suspender o interrumpir la utilización o comunicación de los datos. En los Lineamientos se establece el procedimiento para la aplicación de este artículo.

En cuanto a los sistemas de datos personales en materia de salud, la Ley establece un régimen de excepción en cuanto a su tratamiento, el cual se regirá por lo dispuesto en la Ley General de Salud, la Ley de Salud para el Distrito Federal y demás normas que de ellas deriven.[29]

Sin embargo, se establece la obligación de preservar los datos de identificación personal del paciente, separados de los de carácter clínico-asistencial, de manera tal que se mantenga la confidencialidad de

los mismos, salvo que el propio paciente haya dado su consentimiento para no separarlos. Se exceptúan los supuestos de investigación científica, de salud pública o con fines judiciales, en los que se considere imprescindible la unificación de los datos identificativos con los clínico-asistenciales.[30]

En la Ley se establece una manifestación del principio de temporalidad de los datos que se refiere a la cancelación de los mismos cuando concluyan los plazos de conservación establecidos en las disposiciones aplicables o cuando dejen de ser necesarios para los fines para los que fueron recabados (artículo 19).

En tanto que en los Lineamientos se prevé que los datos personales que hayan sido objeto de tratamiento y no contengan valores históricos, científicos o estadísticos, deberán ser cancelados del sistema de datos personales, teniendo en cuenta los siguientes plazos:

a) El que se haya establecido en el formato físico o electrónico por medio del cual se recabaron.

b) El establecido por las disposiciones aplicables.

c) El establecido en el instrumento jurídico formalizado entre un tercero y el ente público.

Finalmente, dentro del apartado relativo al tratamiento de datos personales, cabe abordar lo relativo a las cesiones de datos, entendiendo por **cesión**:

> ...toda obtención de datos resultante de la consulta de un archivo, registro, base o banco de datos, una publicación de los datos contenidos en él, su interconexión con otros ficheros y la comunicación de datos realizada por una persona distinta a la interesada, así como la transferencia o comunicación de datos realizada entre entes públicos.

En los Lineamientos se prevé que la cesión de datos personales sólo podrá realizarse cuando el cesionario garantice por escrito un nivel de protección similar al empleado en el sistema de datos personales. Así mismo existe la obligación de presentar un informe anual de datos sobre el particular.

Tema 7. Obligaciones de los Entes Públicos

La primera obligación a cumplir por parte de los entes públicos recae sobre el titular del mismo, ya que es quien debe designar al ***responsable de los sistemas de datos personales***. La Ley y los Lineamientos definen al Responsable de los Sistemas de Datos Personales como:

Ley	Lineamientos
La persona física que decida sobre su protección y tratamiento, así como el contenido y finalidad de los sistemas	El servidor público de la unidad administrativa a la que se encuentre adscrito el sistema de datos personales, designado por el titular del ente público, que decide sobre el tratamiento de datos personales, así como el contenido y finalidad de los sistemas de datos personales

La definición contenida en los lineamientos, es un reflejo de lo que dispone la Ley en su artículo 22 donde se prevé que el titular puede delegar la atribución de decidir sobre la finalidad, contenido y uso del tratamiento de datos personales en la unidad administrativa en la que esté adscrito el responsable y el propio sistema de datos.

El responsable del sistema de datos personales tiene, entre sus obligaciones, la de adoptar las medidas necesarias para evitar una vulneración en cualquiera de los principios de protección de datos y debe asegurarse que toda persona que intervenga en el tratamiento de datos del sistema bajo su responsabilidad los conozca y respete.

Las obligaciones a observar **por parte de los responsables** de sistemas de datos personales están previstas en el artículo 21 de la Ley, entre las que destacan:

- ❒ Cumplir políticas y lineamientos para el tratamiento de datos personales.
- ❒ Adoptar las medidas de seguridad y comunicar al InfoDF el nivel de seguridad aplicable para su registro.
- ❒ Presentar un informe anual sobre el cumplimiento de la Ley.

- ❒ Adoptar procedimientos para el trámite de los derechos ARCO y capacitar para su atención y seguimiento.
- ❒ Actualizar datos personales de oficio.
- ❒ Establecer criterios específicos sobre medidas de seguridad, así como un plan de capacitación.
- ❒ Resolver sobre el ejercicio de derechos ARCO.

En el tratamiento de datos personales no sólo interviene el responsable, sino que al interior del ente público y para el cumplimiento de sus funciones, son otras personas las que cotidianamente utilizan datos personales para el desarrollo de su labor, sin que esta utilización implique una delegación de responsabilidad. A estas personas se les define en los Lineamientos bajo la figura de **encargado**.

En tanto que el **usuario** es aquella persona física o moral externa al ente público que le presta servicios para tratar datos personales o que implica el tratamiento de los mismos.

En estos casos, el responsable deberá asegurarse que el tratamiento de datos personales esté regulado en un contrato por escrito o en alguna otra forma que permita acreditar su celebración y contenido.

En este contrato debe estipularse que el usuario:

- ❒ Únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento.
- ❒ No aplicará o utilizará los datos con una finalidad distinta a la que figura en el contrato.
- ❒ No comunicará los datos a otras personas.
- ❒ Adoptará las medidas de seguridad que se deban implementar para su tratamiento.

Los órganos de control de protección de datos han sido creados con el objetivo de asegurar el cumplimiento de la legislación en la materia y, por ende, el respeto al derecho de los ciudadanos

Concluida la relación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable.

Por otra parte, en los Lineamientos se inserta la figura de **enlace** que se define como**:**

> ...el servidor público designado por el titular que fungirá como vínculo, entre el ente público y el Instituto, en materia de protección de datos personales, quien, entre otras obligaciones, coordinará a los distintos responsables de sistemas dentro del ente y remitirá el informe a que hace referencia el artículo 21 de la Ley.

El informe que deben presentar los entes públicos a más tardar el último día hábil del mes de enero de cada año debe contener los siguientes rubros:

1) Número de solicitudes de acceso, rectificación, cancelación y oposición de datos personales presentadas ante el ente público, así como su resultado.
2) Tiempo de respuesta a la solicitud.
3) Estado de las denuncias presentadas ante los órganos internos de control, así como de las vistas dadas por el Instituto.
4) Dificultades observadas en el cumplimiento de la Ley.
5) Descripción de los recursos públicos utilizados en la materia.
6) Sistemas de datos personales creados, modificados y/o suprimidos.
7) Acciones de capacitación.

Dentro del catálogo de obligaciones de los entes públicos, no se encuentra claramente establecida la que se refiere al deber de secrecía, la cual constituye un principio fundamental en la protección de datos. Sin embargo, sí está prevista en el artículo 5 de la Ley en relación con el principio de confidencialidad.

Tema 8. Instituto de Acceso a la Información Pública del Distrito Federal

Los órganos de control de protección de datos han sido creados con el objetivo de asegurar el cumplimiento de la legislación en la materia y, por ende, el respeto al derecho de los ciudadanos.

El control es aquella actividad desplegada con el fin de comprobar, inspeccionar o fiscalizar un desempeño y que constituye un quehacer indispensable en todo sistema jurídico organizado.

Las leyes que existen sobre la materia normalmente atribuyen a las autoridades de control ciertas facultades tales como ordenar medidas cautelares, conferir o negar autorización para tratar determinada categoría de datos, así como ordenar la implementación de medidas de seguridad específicas y, en algunos casos, están dotadas de amplias facultades sancionadoras.[31]

En la Ciudad de México, el Instituto de Acceso a la Información Pública del Distrito Federal (InfoDF), es el encargado de dirigir y vigilar el cumplimiento de la Ley de Protección a Datos Personales del Distrito Federal (LPDPDF), así como de las normas que de ella deriven.

Recordemos que el InfoDF es un órgano autónomo creado por la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal y cuenta con personalidad jurídica y patrimonio propios, autonomía presupuestaria de operación y de decisión en materia de transparencia y acceso a la información pública.

Cualquier persona puede ejercitar los derechos de acceso, rectificación, cancelación y oposición sobre datos de carácter personal que le conciernan tratados por los entes públicos

El InfoDF es ahora al mismo tiempo, la autoridad encargada de garantizar la protección y el correcto tratamiento de datos personales con la atribución de establecer, en el ámbito de su competencia, políticas y lineamientos de observancia general para el manejo, tratamiento, seguridad y protección de los datos personales que estén en posesión de los entes públicos, así como expedir aquellas normas que resulten necesarias para su cumplimiento.

Fruto del ejercicio de esa atribución es la emisión, por parte del Instituto, de los Lineamientos para la Protección de Datos Personales en el Distrito Federal que hemos venido analizando a lo largo de este documento que, también, es producto de las atribuciones legales conferidas por la Ley al InfoDF.

Pero la Ley no sólo faculta al Instituto para establecer normas, sino también le otorga otras atribuciones (artículo 24) con el fin de que sea capaz de garantizar el derecho a la protección de los datos personales en posesión de los entes públicos del Distrito Federal. Dentro de éstas destacan:

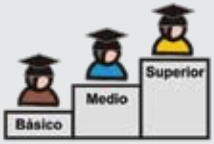
- ❒ Diseñar los formatos y sistema electrónico para solicitudes de derechos ARCO.

Difusión, asistencia y promoción

De las disposiciones legales y reglamentarias al tratamiento de datos personales

Creando archivos

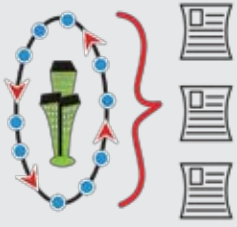
En educación



En formación

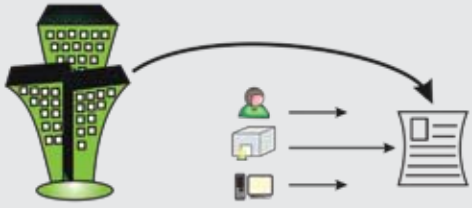
Registro

De los sistemas de datos personales en posesión de los entes públicos



Inspección

Requerir informes y antecedentes de los responsables de sistemas de datos personales, así como del ingreso y registro de establecimientos y equipos en que se realizan las operaciones



Facultades cautelares

Decretar la suspensión temporal en la utilización o cesión de datos, inmovilización de un sistema de datos personales o bloqueo de determinados datos

Facultades normativas

Emitir disposiciones reglamentarias o dictámenes y pronunciamientos específicos

Facultad revisora

Es la instancia ante la cual los particulares pueden presentar un recurso de revisión si consideran que la respuesta a su solicitud de un derecho ARCO les agravia

- ❒ Establecer el registro de sistemas de datos personales en posesión de los entes públicos y mantener actualizado el de niveles de seguridad.
- ❒ Emitir opiniones, observaciones y recomendaciones derivadas de incumplimiento a los principios.
- ❒ Solicitar informes a los entes y presentarlo a la ALDF.
- ❒ Asesoría, investigación, seminarios, capacitación, guías, promoción para difundir el conocimiento de la Ley.
- ❒ Promover en las instituciones educativas la inclusión dentro de sus actividades académicas de los temas que ponderen la importancia de la protección de datos personales.
- ❒ Resolver el recurso de revisión y, en su caso, dar vista al órgano interno de control.
- ❒ Conciliar intereses de particulares con los de entes públicos.
- ❒ Realizar visitas de inspección de oficio a los entes públicos para verificar el cumplimiento de los principios.[32]

Mediante los derechos ARCO, toda persona tiene derecho a que se le informe gratuitamente del origen de sus datos

En los siguientes párrafos, se presenta una breve sistematización de las **atribuciones del Instituto** en materia de protección de datos personales:

1) **Difusión**, **asistencia y promoción**. El InfoDF es responsable de la difusión de las disposiciones legales y reglamentarias aplicables al tratamiento de datos personales. Además de brindar asistencia tanto a los titulares de datos como a los responsables de los sistemas que los contienen. A esta tarea, se suma la de realizar acciones de promoción en la materia, por ejemplo, mediante el desarrollo de eventos que fomenten la profesionalización de los servidores públicos sobre la protección de datos personales.

2) **Registro**. Es responsable de llevar un registro de los sistemas de datos personales en posesión de los entes públicos, quienes deben notificar al Instituto la creación, modificación o supresión de sistemas de datos personales.

3) **Inspección**. Está dotado de facultades de inspección, las que incluyen el requerimiento de informes y antecedentes de los responsables

de sistemas de datos personales, así como el ingreso y registro de los establecimientos y equipos en que se realizan las operaciones. Por su parte, los inspectores quedan obligados a guardar confidencialidad con respecto a la información a que acceden con motivo del ejercicio de las facultades fiscalizadoras; y, en contrapartida, la obstrucción al desempeño fiscalizador —negativa a suministrar información, proporcionar información falsa y resistencia al acceso, entre otras— constituye una infracción a la ley y faculta a la autoridad correspondiente para imponer sanciones de naturaleza administrativas a los responsables.

4) **Facultades cautelares**. Dispone de facultades excepcionales para adoptar medidas cautelares -tales como decretar la suspensión temporal en la utilización o cesión de datos, la inmovilización de un sistema de datos personales, o el bloqueo de determinados datos- en casos graves en que exista un riesgo real o inminente para los derechos del o los titulares de los datos personales.

5) **Facultades normativas**. Tiene facultades normativas, ya sea de orden general, que se concreta en disposiciones reglamentarias, o bien particular, mediante la emisión de dictámenes y pronunciamientos específicos.

6) **Facultad revisora**. Es la instancia ante la cual los particulares pueden presentar un recurso de revisión si consideran que la respuesta a su solicitud de un derecho ARCO les agravia. Las resoluciones que emita serán definitivas, inatacables y obligatorias.

Tema 9. Derechos ARCO y Procedimiento para su Ejercicio

Un aspecto fundamental de los sistemas jurídicos en materia de protección de datos lo constituye el establecimiento en las leyes de los denominados derechos ARCO:

A. Acceso.
R. Rectificación.
C. Cancelación.
O. Oposición.

La posibilidad de ejercer estos derechos es lo que dota a la persona de una verdadera facultad de disposición sobre sus propios datos personales, ya que mediante ellos:

- ❒ Puede conocer qué datos tienen los entes públicos.
- ❒ Rectificarlos en caso de errores.
- ❒ Cancelarlos si dejaron de ser necesarios.
- ❒ Oponerse a su tratamiento si es que fueron obtenidos sin su consentimiento.

La Ley establece la posibilidad de ejercer los derechos ARCO a toda persona, y precisa que se trata de derechos independientes, por lo que el ejercicio de alguno no es condicionante ni impedimento para ejercer otro.

Por tanto, cualquier persona puede ejercitar los derechos de acceso, rectificación, cancelación y oposición sobre datos de carácter personal que le conciernan tratados por los entes públicos. Un requisito indispensable para el ejercicio de estos derechos es la identificación del interesado o, en su caso, la de su representante legal.

Mediante los derechos ARCO, toda persona tiene derecho a que se le informe gratuitamente del origen de sus datos y a saber a qué otras personas o entidades, sean de derecho público o privado, han sido comunicados. Este derecho se complementa con el de rectificar la información incorrecta o no actualizada, con

CUALQUIER PERSONA PUEDE EJERCER LOS DERECHOS ARCO

el derecho a solicitar que se destruyan aquellos datos que sean inexactos o incompletos, o aquéllos que no cumplan el principio de adecuación con la finalidad para la que fueron recabados.

A continuación describiremos cada uno de estos derechos ARCO:

Derecho de Acceso. Nos permite solicitar y obtener información de nuestros datos personales sometidos a tratamiento, la finalidad, su origen, así como las comunicaciones realizadas o previstas.

Asimismo, nos permite obtener datos concretos, así como los datos incluidos en un determinado sistema o la totalidad de los datos sometidos a tratamiento en los sistemas de datos personales en posesión de un ente público.

Derecho de Rectificación. Nos otorga la facultad de solicitar que se modifiquen los datos que resulten inexactos o incompletos con respecto a la finalidad para la cual fueron obtenidos. Los datos deben ser considerados exactos cuando:

1) Corresponden a nuestra situación actual.
2) Reflejen hechos constatados en un procedimiento administrativo o judicial.

Derecho de Cancelación. Procede cuando nuestros datos son inadecuados o excesivos:

1) *Inadecuados* cuando no guardan relación con el ámbito de aplicación y finalidad por la cual fueron recabados, o bien, si dejaron de ser necesarios con respecto a dicha finalidad.
2) *Excesivos*, si los datos obtenidos son más de los estrictamente necesarios en relación a dicha finalidad.

La cancelación también procede cuando el tratamiento de nuestros datos personales no se ajuste a lo dispuesto en la Ley o en los Lineamientos.

Aquí cabe recordar el principio de calidad que determina que, los datos personales recabados deben ser ciertos, adecuados, pertinentes y no excesivos con relación al ámbito y finalidad para los que fueron obtenidos.

La cancelación no implica la desaparición física del dato de modo tal que no permita su recuperación posterior, sino que existe un paso intermedio en el que se bloquea el dato y sólo permanece accesible para algunos y en determinadas circunstancias, como es el caso de autoridades públicas y jurisdiccionales para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante los plazos de prescripción aplicables.

Pensemos, por ejemplo, en la responsabilidad administrativa, la cual tiene plazos de prescripción para imponer sanciones que van desde los tres hasta los cinco años, por lo que los datos relacionados con este tema tienen que conservarse hasta que ese tiempo transcurra.[33]

Derecho de Oposición. Actúa cuando los datos fueron recabados sin nuestro consentimiento. Ante este supuesto, podemos solicitar que no se lleve a cabo el tratamiento de nuestros datos personales para un fin determinado o se cese en el mismo. En caso de que la oposición sea procedente, esta dará lugar a la cancelación del dato.

Derecho de cancelación: Procede cuando nuestros datos son inadecuados o excesivos

Es importante tener en cuenta que tanto la cancelación, como la oposición, de ser procedentes, dan lugar al bloqueo de los datos.

El *bloqueo de datos* consiste en la conservación de datos personales con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo, legal o contractual, de prescripción de éstas. Durante este periodo, los datos personales no pueden ser objeto de tratamiento y transcurrido éste, se procede a su eliminación del sistema.

Lo mismo sucede en caso de que sea procedente la revocación del consentimiento que tratamos anteriormente.

En caso de que se realice cualquier rectificación o cancelación sobre unos datos que previamente fueron cedidos, el responsable tendrá que notificar al cesionario dicha actuación para que éste a su vez efectúe las operaciones correspondientes sobre los datos cedidos.

Los derechos ARCO no son absolutos, por lo que el responsable del sistema de datos personales podrá denegarlos cuando exista una causa legal o justificada para ello.

En este sentido, no procede la rectificación si se trata de datos que:

- ❒ Reflejen hechos que formen parte de un procedimiento administrativo o un proceso judicial.
- ❒ Resulte imposible o exija esfuerzos desproporcionados, como podría ser el caso de una solicitud para que se corrijan datos de un expediente laboral de 1980 que ya no se encuentre en los archivos del ente público.

Puede denegarse la cancelación cuando:

- ❒ Exista un deber de conservación de los datos.
- ❒ Pudiera afectar derechos o intereses legítimos de otras personas, como lo es el propio Estado. En este sentido, se puede negar la cancelación de datos por motivos de seguridad pública.

Procedimiento ejercicio derechos ARCO:

En relación con este apartado diremos en primera instancia que la aplicación cotidiana de cualquier instrumento jurídico requiere del establecimiento de un procedimiento preciso y claro que facilite la concreción, en el terreno de lo práctico, de los preceptos y fundamentos que tutela.

En este sentido, el procedimiento para el ejercicio de los derechos ARCO establecido en la Ley y los Lineamientos señala los instrumentos y mecanismos para dar cumplimiento a esta necesidad. Se refiere tanto a lo que debe cubrir el interesado como a lo que los servidores públicos de los entes están obligados a realizar para atender las solicitudes en esta materia.

Instancia ante la que se presenta la solicitud:

Todos los entes públicos cuentan con una unidad administrativa denominada “Oficina de Información Pública (OIP)”, que es la encargada, entre otras funciones, de recibir las solicitudes para el ejercicio de tus derechos ARCO.

Medios de Acceso:

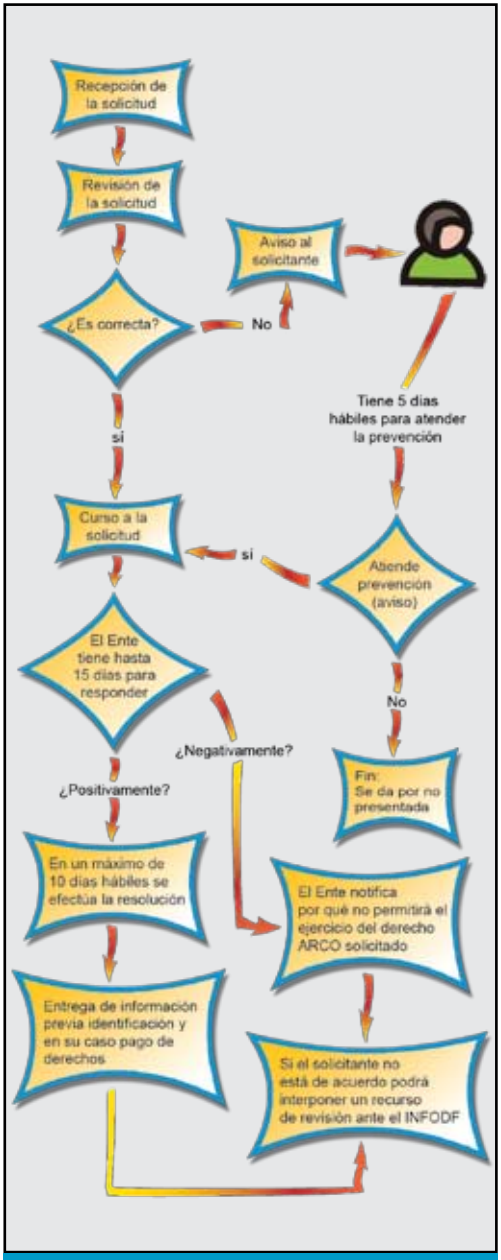
Recordemos que estos derechos ARCO sólo los puede ejercer el titular de los datos (interesado), o en su caso, su representante legal. Existen diversos medios para la presentación de una solicitud ante la OIP correspondiente:

1) Por **escrito material** ante la OIP, o enviado por correo ordinario, certificado o mensajería.
2) **Verbal**, de manera oral y directa, la cual será capturada por el responsable de la OIP en el formato respectivo e ingresada al sistema INFOMEX-DF.
3) **Correo electrónico** a la dirección de correo electrónico asignada a la OIP.
4) Por el sistema electrónico **INFOMEX-DF**.
5) Vía telefónica, al 5636-4636, a través del servicio **TELINFODF**.

Requisitos:

A fin de que el Ente te atienda de la forma adecuada, en cualquiera de los medios de acceso disponibles, es necesario que en tu solicitud proporciones los siguientes datos:

1) **Ente público** a quien diriges la solicitud.
2) Tu **nombre completo** y, en su caso, el de tu representante legal.
3) **Descripción** clara y precisa **de los datos** personales respecto de los que buscas ejercer algún derecho ARCO.
4) Cualquier **otro elemento** que facilite su **localización**.
5) El **domicilio,** mismo que se debe encontrar dentro del **Distrito Federal**, u otro **medio** para recibir notificaciones (correo electrónico, OIP, si no lo indicas se te notificará por estrados).



PROCEDIMIENTO DE LOS DERECHOS ARCO

Además de estos requisitos, existen algunos otros que son específicos del derecho que vayas a ejercer:

- **Derecho de Acceso**: Indicar la modalidad en la que prefiere se otorgue el acceso que puede ser consulta directa, copias simples o certificadas.
- **Derecho de Rectificación**: Señalar el dato erróneo y la corrección que deba realizarse, acompañado de la documentación que lo avale.
- **Derecho de Cancelación**: Indicar las razones por las cuales se considera que el tratamiento de los datos no se apega a las disposiciones normativas.
- **Derecho de Oposición**: Señalar los motivos por los que no se está de acuerdo en el uso o difusión de los datos.

Si sucede que tu solicitud no es clara o no cumple con todos los requisitos que ya te mencionamos, la OIP puede, dentro del plazo de cinco días después de recibida tu solicitud, pedirte que corrijas las deficiencias que detectó. Si este es el caso, tendrás cinco días para hacerlo, de lo contrario, la OIP no dará trámite a tu solicitud, pues se tendrá por no presentada. Cabe precisar que este requerimiento interrumpe el plazo para dar respuesta.

Tiempos y tipo de respuesta:

Una vez que la OIP recibe tu solicitud mediante cualquiera de los medios previstos, se realiza un proceso interno de análisis para determinar la aceptación o rechazo de la misma. El ente público cuenta con un plazo de quince días hábiles para responderla, aunque debes considerar que este plazo puede ampliarse por un periodo igual, si existe alguna causa justificada para ello.

La respuesta a tu solicitud puede ser:

- *Procedente*, esto es decir, el ente te estará dando una respuesta positiva a la petición que hiciste, y deberá hacerlo de tu conocimiento a través del medio que indicaste para recibir

notificaciones. La determinación se hará efectiva dentro de los siguientes diez días.

- ❒ *No procedente*, significa que te han negado la petición que hiciste y la respuesta que te den debe especificar las razones y las normas jurídicas aplicables que determinaron la negativa. Esta respuesta debe estar suscrita y firmada por el responsable del sistema y por el titular de la OIP del ente público que corresponda, pudiendo recaer ambas funciones en la misma persona.

En caso de que los datos personales sobre los cuales estás solicitando ejercer un derecho ARCO no se localicen en los sistemas del ente, se elaborará un acta, misma que se hará de tu conocimiento dentro del plazo de respuesta. En esta acta, se dará cuenta de los sistemas en que fueron buscados tus datos personales y deberá estar firmada por un representante del órgano interno de control, del titular de la OIP y del responsable del sistema de datos personales.

Acreditación de tu identidad para recibir la respuesta:

Es importante que recuerdes que independientemente del medio a través del cual se reciba tu solicitud, es necesario que acredites tu identidad o, en su caso, la personalidad, identidad y facultades de tu representante legal, esto debe hacerse en el momento que te presentes en la OIP correspondiente para obtener la respuesta sobre la solicitud de tus datos personales.

El InfoDF es el órgano garante de hacer cumplir la Ley. Ante el caso de una violación a alguna de sus disposiciones, se debe presentar un escrito denominado "recurso de revisión"

Para acreditar tu identidad o la de tu representante legal, debes presentar cualquier documento oficial en original como:

- ❒ Credencial para votar.
- ❒ Pasaporte vigente.
- ❒ Cartilla del servicio militar.
- ❒ Cédula profesional.
- ❒ Credencial de afiliación al Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado (ISSSTE), al Instituto Mexicano del Seguro Social (IMSS) o al Instituto Nacional de Personas Adultas Mayores (INAPAM).

Del pago de derechos:

La Ley establece que el trámite de la solicitud es gratuito, lo cual constituye un principio comúnmente adoptado en las leyes sobre la materia. Sin embargo, se prevé que el solicitante debe cubrir los costos de reproducción de los datos solicitados según lo previsto en el Código Financiero.

Estos derechos se cobrarán previo a la entrega de la información y se calcularán atendiendo a los costos de los materiales, del envío y, en su caso, de la certificación de documentos.

Tema 10. Recurso de Revisión

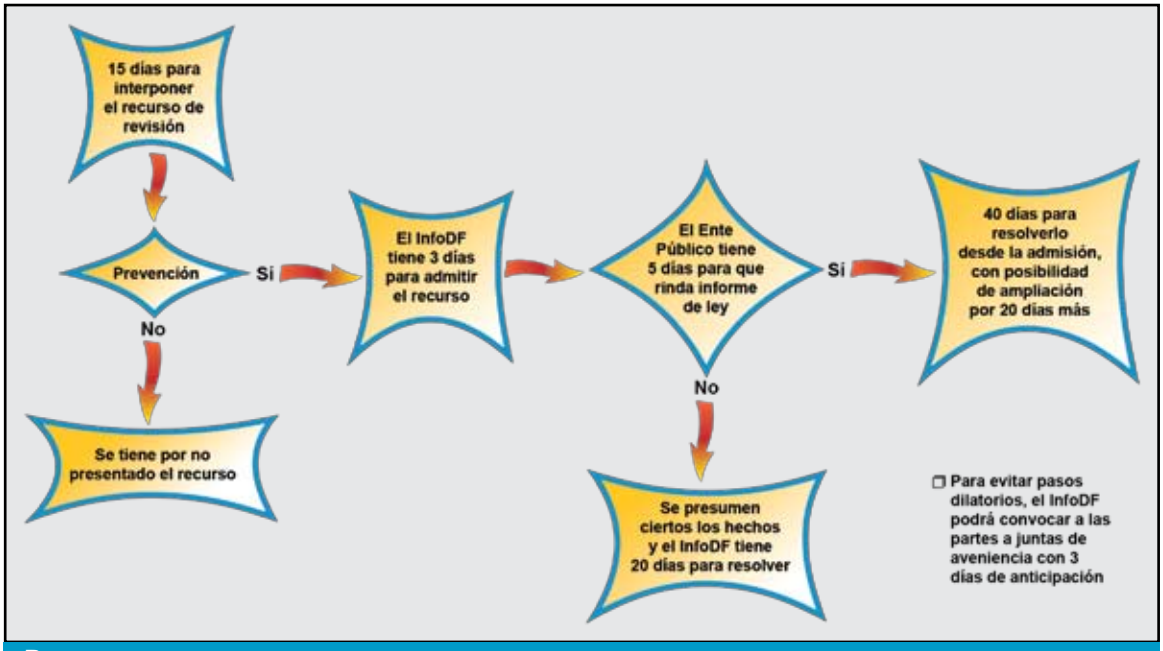
Primero que nada es conveniente definir qué es un *recurso administrativo*, ya que el recurso de revisión que puede interponerse ante el Instituto de Acceso a la Información Pública del Distrito Federal es un ejemplo de este tipo de recursos.

Un recurso administrativo es un medio de defensa con el que cuenta un ciudadano en contra de los actos de autoridad que considere ilegales y que le causen un agravio específico; se interpone ante el mismo órgano de autoridad, su superior jerárquico o la instancia que determine la Ley, para que ese acto sea revocado (es decir, dejado sin efectos) o bien modificado.

Cabe señalar que el órgano que resuelve el recurso también puede confirmar el acto que se impugna o recurre. Como el InfoDF es el órgano garante de hacer cumplir la Ley, ante el caso de una violación a alguna de sus disposiciones, se debe presentar un escrito denominado "recurso de revisión".

El recurso de revisión es el medio de defensa con el que cuentan las personas que se consideren agraviadas con la respuesta que haya recaído a su solicitud para ejercer cualquiera de los derechos ARCO o ante la omisión de la misma.

La OIP, tiene la obligación de informarte, en la respuesta a tu solicitud, sobre el derecho que tienes a presentar un recurso de revisión, así como el modo y plazo que tienes para hacerlo.



Procedimiento para el recurso de revisión

Independientemente al recurso de revisión, y en caso de que lo consideres pertinente, también tienes derecho a presentar una queja ante el órgano interno de control correspondiente.

La LPDPDF prevé que el recurso de revisión se tramite de conformidad con el procedimiento previsto en la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal (LTAIPDF), del cual haremos un breve repaso.[34]

Requisitos:

El recurso de revisión se interpone por escrito o por medio electrónico dentro de los 15 días hábiles contados a partir de la fecha en que surta efectos la notificación de la resolución con la cual no se está de acuerdo.

Ahora bien, si el recurso de revisión se presenta por falta de respuesta del Ente Público, el plazo para presentarlo se cuenta a partir del momento en que concluye el periodo que tenía el Ente para dar

contestación a la solicitud, en este caso, basta que el solicitante acompañe al recurso el documento que pruebe la fecha en que presentó la solicitud.

El recurso de revisión debe cumplir los siguientes requisitos, de acuerdo con lo que señala el **artículo 78** de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal:

- ❒ Dirigirse al Instituto de Acceso a la Información Pública del D. F.
- ❒ Contener el nombre del inconforme o representante legal y el nombre del tercero interesado o afectado en su caso.
- ❒ El domicilio o medio electrónico para oír y recibir las notificaciones.
- ❒ Precisar el acto que se impugna y la autoridad responsable.
- ❒ Señalar la fecha en la que se le notificó al solicitante el acto o resolución que se impugna.
- ❒ Mencionar los hechos y agravios que le causa el acto al solicitante, y los artículos violados.
- ❒ Acompañar copia de la resolución correspondiente o copia de la iniciación del trámite.

Un recurso administrativo es un medio de defensa con el que cuenta un ciudadano en contra de los actos de autoridad que considere ilegales y que le causen un agravio específico

Los “agravios” los podemos entender como la aplicación indebida de las disposiciones de la Ley de Protección de Datos Personales para el Distrito Federal u otros ordenamientos legales que el recurrente (persona afectada que presenta un recurso de revisión) considera cometió la autoridad responsable al emitir la resolución que se impugna, o bien la falta de respuesta.

Si se da el caso de que el recurrente no cumple con alguno de los requisitos mencionados, el Instituto, en un plazo no mayor a cinco días, lo prevendrá para que en un periodo de cinco días hábiles corrija las irregularidades encontradas.

Procedimiento:

Una vez presentado el recurso, el Instituto tiene hasta 40 días[35] para emitir una resolución a través del siguiente procedimiento:

1) El InfoDF revisa y emite el acuerdo de correspondiente (puede ser de admisión, prevención o desechamiento) dentro de los 3 días hábiles siguientes.

   En caso de no cumplir con alguno de los requisitos establecidos, el InfoDF puede solicitarte que corrijas las deficiencias en un lapso máximo de 5 días hábiles (prevención).

   En este caso también se tienen 5 días hábiles para hacerlo. Si no lo haces, se tendrá por no presentado tu recurso.

2) Admitido el recurso, el InfoDF solicita al ente público que rinda un informe sobre la situación, dentro de los 5 días hábiles siguientes.
3) En caso de existir tercero interesado, se le dará vista para que en el mismo plazo acredite su carácter y manifieste lo que a su derecho convenga.
4) El informe del ente se hará del conocimiento del recurrente para que presente pruebas y manifieste lo que considere conveniente, en un plazo de 5 días hábiles.
5) Las partes tienen 3 días hábiles para presentar sus alegatos.
6) Finalmente en una sesión pública, el Pleno del InfoDF emite la resolución respectiva y ordena su notificación al recurrente, al ente público correspondiente, así como al tercero interesado, en su caso. La resolución deberá ser por escrito y contener el plazo y los procedimientos para su cumplimiento.

En algunos casos, el InfoDF podrá convocar, con 3 días hábiles de anticipación, al ente público y al recurrente a efecto de reunirse y evitar pasos dilatorios en la entrega de la información.

Tipos de resolución:

El Instituto puede resolver los recursos en estos sentidos:

- ❒ Desechar el recurso.
- ❒ Sobreseerlo, es decir, dar por terminado su trámite.
- ❒ Confirmar la respuesta que haya emitido el Ente Público.

- ❒ Revocar o modificar la respuesta del Ente Público y ordenarle que:
  - a) Permita el acceso a los datos solicitados.
  - b) Rectifique los datos.
  - c) Cancele los datos.

Las resoluciones del Instituto son definitivas, inatacables —es decir, no se pueden impugnar, salvo a través del juicio de amparo— y obligatorias para los particulares y para los entes públicos. En el texto de las resoluciones se debe hacer mención a qué instancia puede acudir el inconforme en defensa de sus derechos constitucionales (en este caso ante un juez de distrito, en demanda de amparo indirecto).

El Ente que haya recibido una resolución del Instituto está obligado a cumplirla y a informar sobre su cumplimiento en un plazo no mayor a cinco días hábiles, en caso contrario, el Instituto debe notificar al superior jerárquico del Ente Público responsable, a fin de que ordene el cumplimiento en un plazo que no debe exceder de diez días. Si se diera el caso de que persistiera el incumplimiento, se notificará al órgano interno de control para su inmediata intervención e inicie el procedimiento de responsabilidad correspondiente.

Tema 11. Infracciones

Las infracciones constituyen mecanismos coercitivos para exigir el cumplimiento de las leyes.

Infracción. Se entiende por infracción a la transgresión, quebrantamiento, violación, incumplimiento de ley, reglamento, convenio, tratado, contrato u orden.

La LPDPDF dedica su Título Quinto “De las Responsabilidades” a establecer, en un Capítulo Único, las infracciones a la Ley, como son:

- ❒ Omisión o irregularidad en la atención de solicitudes ARCO.
- ❒ Recabar datos personales sin cumplir con el deber de Información o sin el consentimiento cuando éste es procedente.
- ❒ Crear sistemas sin la publicación correspondiente en la GODF.

- ❒ Incumplir con los principios, con las resoluciones del InfoDF o con la presentación del informe.
- ❒ Obtención fraudulenta o engañosa de datos; transmisiones indebidas (lucro).
- ❒ Obstaculizar inspección del InfoDF.
- ❒ Destruir, alterar o ceder datos personales sin autorización.

Estas infracciones o cualquiera otra derivada del incumplimiento de las obligaciones establecidas en la Ley, será sancionada en términos de la Ley de Federal de Responsabilidades de los Servidores Públicos. Las sanciones son independientes de las de orden civil o penal que procedan, así como los procedimientos para el resarcimiento del daño ocasionado por el ente público.

Por otra parte, se da atribución al Instituto para denunciar cualquier infracción a la Ley ante las autoridades competentes y podrá aportar las pruebas que considere convenientes.

En este último apartado se establece la obligación, hacia los órganos internos de control y fiscalización de los entes públicos, de entregar un informe estadístico semestral sobre procedimientos administrativos iniciados por incumplimiento a la LPDPDF y sus resultados, información que debe ser incorporada al informe anual que presenta el Instituto a la Asamblea Legislativa.

Las resoluciones que se adopten sobre el particular deben ser notificadas al ente público, al responsable del sistema de datos personales y, en su caso, a los interesados.

Las infracciones constituyen mecanismos coercitivos para exigir el cumplimiento de las leyes

Síntesis

La protección de datos personales es un derecho que consiste en ofrecer a los individuos los medios jurídicos necesarios para controlar el uso de la información personal que les concierne.

La LPDPDF, a efecto de garantizar la debida protección de los mismos, además de establecer los derechos ARCO, incluye una serie de principios rectores en el tratamiento de este tipo de datos, como son el de finalidad, calidad, consentimiento, deber de información, seguridad, confidencialidad, disponibilidad y temporalidad.

Asimismo, la Ley establece la obligación, por parte de los entes públicos, de que los datos organizados en sus archivos, registros, ficheros, bases o bancos de datos personales —denominados en la Ley como sistemas de datos personales— deban contar con medidas y tipos de seguridad, en atención a la sensibilidad de los datos contenidos en cada sistema.

De igual forma, los entes públicos deben realizar el tratamiento de los datos estrictamente necesarios para el ejercicio de sus atribuciones, atendiendo a una serie de obligaciones, que reflejan la observancia de los principios básicos de la protección de datos, como lo son (i) informar al interesado con carácter previo al tratamiento de datos; (ii) recabar sólo los datos imprescindibles para el ejercicio de sus atribuciones; y (iii) facilitar a las personas el ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO).

En este sentido, todas aquellas personas que de alguna forma se relacionen con el tratamiento de los datos personales y, en particular el responsable del sistema, deben cumplir con ciertas obligaciones, entre las que se encuentran: guardar confidencialidad de los datos que

manejan en el ejercicio de sus funciones; presentar un informe anual sobre el cumplimiento de la Ley; actualizar los datos personales de oficio; establecer criterios específicos sobre medidas de seguridad, así como elaborar un plan de capacitación y resolver sobre el ejercicio de derechos ARCO.

Ahora bien, los titulares de los datos personales, cuentan con el derecho de recurrir ante el Instituto de Acceso a la Información Pública del Distrito Federal (InfoDF) -órgano garante del derecho de acceso a la información pública, y de la protección de los datos personales, cuando se consideren agraviados por la respuesta que haya recaído a su solicitud para ejercer cualquiera de los derechos ARCO o ante la omisión de la misma, lo anterior a través de un recurso de revisión.

El procedimiento para el ejercicio de los derechos ARCO se hará de conformidad con lo dispuesto en la LPDPDF; los Lineamientos para la Gestión de Solicitudes de Información Pública y de Datos Personales a través del Sistema INFOMEX-DF; y los Lineamientos para la Protección de Datos Personales en el Distrito Federal.

Finalmente debemos señalar que la Ley contiene un capítulo relativo a las infracciones que, derivadas del incumplimiento de la LPDPDF, pueden existir, las cuales serán aplicadas por el Órgano Interno de Control correspondiente y atenderán a las sanciones establecidas en la Ley Federal de Responsabilidades de los Servidores Públicos, siendo éstas independientes de las sanciones civiles y/o penales que pudieran presentarse.

AUTOEVALUACIÓN

AUTOEVALUACIÓN

Cuestionario sobre los contenidos generales del módulo tres, “Aspectos Relevantes de la Ley de Protección de Datos Personales para el Distrito Federal (LPDPDF)”.

1. Constituye un principio en materia de protección de datos personales:

A. Máxima publicidad.
B. Licitud.
C. Derecho de petición.
D. Información reservada.

2. En atención al principio de calidad los datos personales deben ser:

A. Ciertos, adecuados, pertinentes y no excesivos.
B. Históricos, estadísticos o científicos.
C. Secretos.
D. Disponibles.

3. El consentimiento se refiere a la manifestación de la voluntad:

A. Cierta, presente y unívoca.
B. Libre, inequívoca, específica e informada.
C. Veraz, oportuna y pertinente.
D. Secreta, confidencial y reservada.

4. Se considera como un dato sensible:

A. Información patrimonial.
B. Características personales.
C. Datos de origen.
D. B y C.

5. El derecho de protección de datos es:

A. El poder de disposición y control que faculta a su titular a decidir cuáles de sus datos proporciona a un tercero, así como el saber quién posee esos datos y para qué, pudiendo oponerse a esa posesión o uso.
B. El derecho que tiene toda persona de acceder y corregir sus datos.
C. El derecho de manifestar su oposición a cualquier tratamiento.
D. Ninguna de las anteriores.

Anexos

Temario

Entes Públicos

Obligados del Distrito Federal

Órgano Ejecutivo

Administración Pública Centralizada

- Jefatura de Gobierno del Distrito Federal.
  http://www.df.gob.mx/
- Secretaría de Gobierno.
  http://www.sg.df.gob.mx
- Secretaría de Desarrollo Urbano y Vivienda.
  http://www.seduvi.df.gob.mx
- Secretaría de Desarrollo Económico.
  http://www.sedeco.df.gob.mx
- Secretaría de Turismo.
  http://www.mexicocity.gob.mx
- Secretaría del Medio Ambiente.
  http://www.sma.df.gob.mx
- Secretaría de Obras y Servicios.
  http://www.obras.df.gob.mx
- Secretaría de Desarrollo Social.
  http://www.sds.df.gob.mx
- Secretaría de Finanzas.
  http://www.finanzas.df.gob.mx
- Secretaría de Transportes y Vialidad.
  http://www.setravi.df.gob.mx
- Secretaría de Seguridad Pública.
  http://portal.ssp.df.gob.mx
- Secretaría de Salud.
  http://www.salud.df.gob.mx
- Secretaría de Cultura.
  http://www.cultura.df.gob.mx
- Oficialía Mayor.
  http://www.om.df.gob.mx

- Contraloría General del Distrito Federal.
  http://www.contraloria.df.gob.mx
- Procuraduría General de Justicia del Distrito Federal.
  http://www.pgjdf.gob.mx
- Consejería Jurídica y de Servicios Legales.
  http://www.consejeria.df.gob.mx
- Secretaría de Educación.
  http://www.educacion.df.gob.mx
- Secretaría de Desarrollo Rural y Equidad para las Comunidades.
  http://www.sederec.df.gob.mx
- Secretaría de Protección Civil.
  http://www.proteccioncivil.df.gob.mx/
- Secretaría de Trabajo y Fomento al Empleo.
  http://www.styfe.df.gob.mx/

Delegaciones

- Delegación Álvaro Obregón.
  http://www.aobregon.df.gob.mx
- Delegación Azcapotzalco.
  http://www.azcapotzalco.gob.mx
- Delegación Benito Juárez.
  http://www.delegacionbenitojuarez.gob.mx
- Delegación Coyoacán.
  http://www.coyoacan.df.gob.mx
- Delegación Cuajimalpa de Morelos.
  http://www.cuajimalpa.df.gob.mx
- Delegación Cuauhtémoc.
  http://www.cuauhtemoc.df.gob.mx
- Delegación Gustavo A. Madero.
  http://www.gamadero.gob.mx
- Delegación Iztacalco.
  http://www.iztacalco.df.gob.mx
- Delegación Iztapalapa.
  http://www.iztapalapa.gob.mx
- Delegación La Magdalena Contreras.
  http://www.mcontreras.df.gob.mx
- Delegación Miguel Hidalgo.
  http://www.miguelhidalgo.gob.mx
- Delegación Milpa Alta.
  http://www.milpa-alta.df.gob.mx
- Delegación Tláhuac.
  http://www.tlahuac.df.gob.mx

- Delegación Tlalpan.
  http://www.tlalpan.gob.mx
- Delegación Venustiano Carranza.
  http://www.vcarranza.df.gob.mx
- Delegación Xochimilco.
  http://www.xochimilco.df.gob.mx

Desconcentrados, Descentralizados, Paraestatales y Auxiliares

- Autoridad de Espacios Públicos.
  (no tiene página).
- Autoridad del Centro Histórico.
  http://www.autoridadcentrohistorico.df.gob.mx/
- Caja de Previsión de la Policía Auxiliar del Distrito Federal.
  http://www.caprepa.df.gob.mx
- Caja de Previsión de la Policía Preventiva del Distrito Federal.
  http://www.caprepol.df.gob.mx
- Caja de Previsión para Trabajadores a Lista de Raya del Distrito Federal.
  http://www.captralir.df.gob.mx
- Calidad de Vida, Progreso y Desarrollo para la Ciudad de México S. A. de C. V. (Capital en crecimiento)
  http://www.capitalencrecimiento.df.gob.mx
- Comisión de Filmaciones de la Ciudad de México.
  (no tiene página)
- Consejo de Evaluación del Desarrollo Social del Distrito Federal.
  http://www.evalua.df.gob.mx
- Corporación Mexicana de Impresión S. A. de C. V.
  http://www.comisa.df.gob.mx
- Escuela de Administración Pública del Distrito Federal.
  www.escueladeadministracionpublica.df.gob.mx
- Fideicomiso Central de Abasto de la Ciudad de México.
  http://www.ficeda.com.mx/
- Fideicomiso Centro Histórico de la Ciudad de México.
  http://www.centrohistorico.df.gob.mx
- Fideicomiso de Recuperación Crediticia del Distrito Federal.
  http://www.fidere3.df.gob.mx
- Fideicomiso Educación Garantizada del Distrito Federal.
  http://www.fideicomisoed.df.gob.mx/
- Fideicomiso Museo de Arte Popular Mexicano.
  http://www.map.df.gob.mx/
- Fideicomiso Museo del Estanquillo.
  http://www.museodelestanquillo.com

- Fideicomiso para el Fondo de Promoción para el Financiamiento del Transporte Público.
  http://www.setravi.df.gob.mx/
- Fideicomiso para el Mejoramiento de las Vías de Comunicación del Distrito Federal.
  http://www.fimevic.df.gob.mx
- Fideicomiso Público Ciudad Digital.
  www.ciudadmexicodigital.com
- Fideicomiso Público Complejo Ambiental Xochimilco.
  (no tiene página).
- Fideicomiso Público del Fondo de Apoyo a la Procuración de Justicia del Distrito Federal.
  (no tiene página).
- Fondo Ambiental Público del Distrito Federal.
  http://www.sma.df.gob.mx
- Fondo de Desarrollo Económico del Distrito Federal.
  http://www.fondeco.df.gob.mx/
- Fondo de Seguridad Pública del Distrito Federal.
  http://www.pgjdf.gob.mx/foseg/index.php
- Fondo Mixto de Promoción Turística del Distrito Federal.
  http://www.fmpt.df.gob.mx
- Fondo para el Desarrollo Social de la Ciudad de México.
  http://www.fondeso.df.gob.mx
- Fondo para la Atención y Apoyo a las Víctimas del Delito.
  http://www.pgjdf.gob.mx/faavid/index.php
- Heroico Cuerpo de Bomberos del Distrito Federal.
  http://www.bomberos.df.gob.mx
- Instituto de Ciencia y Tecnología del Distrito Federal.
  http://www.icyt.df.gob.mx
- Instituto de Educación Media Superior del Distrito Federal.
  http://www.iems.df.gob.mx
- Instituto de Formación Profesional del Distrito Federal.
  http://www.ifp.pgjdf.gob.mx/
- Instituto de la Juventud del Distrito Federal.
  http://www.jovenes.df.gob.mx
- Instituto Técnico de Formación Policial.
  http://portal.ssp.df.gob.mx
- Instituto de las Mujeres del Distrito Federal.
  http://www.inmujeres.df.gob.mx
- Instituto de Vivienda del Distrito Federal.
  http://www.invi.df.gob.mx
- Instituto del Deporte del Distrito Federal.
  http://www.deporte.df.gob.mx/

- Instituto para la Atención de los Adultos Mayores en el Distrito Federal.
  www.adultomayor.df.gob.mx
- Junta de Asistencia Privada del Distrito Federal.
  http://www.jap.org.mx
- Sistema de Corredores de Transporte Público de Pasajeros del Distrito Federal (Metrobús).
  http://www.metrobus.df.gob.mx
- Sistema de Radio y Televisión Digital del Gobierno del Distrito Federal.
  http://www.canal21.df.gob.mx
- Policía Auxiliar.
  http://portal.ssp.df.gob.mx/Portal/NuestrosPolicias/PoliciaAuxiliar/
- Policía Bancaria e Industrial.
  http://www.policiabancaria.df.gob.mx/
- Procuraduría Ambiental y del Ordenamiento Territorial del Distrito Federal.
  http://www.paot.org.mx
- Procuraduría Social del Distrito Federal.
  http://www.prosoc.df.gob.mx
- Proyecto Metro del Distrito Federal.
  www.proyectometro.df.gob.mx
- Red de Transporte de Pasajeros del Distrito Federal.
  http://www.rtp.gob.mx
- Servicio de Transportes Eléctricos del Distrito Federal.
  http://www.ste.df.gob.mx
- Servicios de Salud Pública del Distrito Federal.
  http://www.salud.df.gob.mx:88/
- Servicios Metropolitanos S. A. de C. V.
  http://www.servimet.df.gob.mx
- Sistema de Aguas de la Ciudad de México.
  http://www.sacm.df.gob.mx
- Sistema de Transporte Colectivo.
  http://www.stc.df.gob.mx
- Sistema para el Desarrollo Integral de la Familia del Distrito Federal.
  http://www.dif.df.gob.mx

Órgano Legislativo

- Asamblea Legislativa del Distrito Federal.
  http://www.asambleadf.gob.mx

- Contaduría Mayor de Hacienda de la Asamblea Legislativa del Distrito Federal.
  http://www.cmhaldf.gob.mx/

Órgano Judicial

- Tribunal Superior de Justicia del Distrito Federal.
  http://www.tsjdf.gob.mx/
- Consejo de la Judicatura del Distrito Federal.
  http://www.cjdf.gob.mx

Órganos Autónomos

- Comisión de Derechos Humanos del Distrito Federal.
  http://www.cdhdf.org.mx
- Instituto de Acceso a la Información Pública del Distrito Federal.
  http://www.infodf.org.mx
- Instituto Electoral del Distrito Federal.
  http://www.iedf.org.mx/
- Junta Local de Conciliación y Arbitraje del Distrito Federal.
  http://www.juntalocal.df.gob.mx/
- Tribunal de lo Contencioso Administrativo del Distrito Federal.
  http://www.tcadf.gob.mx
- Tribunal Electoral del Distrito Federal.
  http://www.tedf.org.mx
- Universidad Autónoma de la Ciudad de México.
  http://www.uacm.edu.mx/

Partidos Políticos del Distrito Federal

- Partido Acción Nacional.
  http://www.df.pan.org.mx
- Partido Revolucionario Institucional.
  http://www.ciudadfutura.org.mx
- Partido de la Revolución Democrática.
  http://www.prddf.org.mx
- Partido del Trabajo.
  http://www.partidodeltrabajo.org.mx/www.ptdf.php
- Partido Verde Ecologista de México.
  http://www.pvem-df.com
- Convergencia.
  http://www.convergenciadfcomite.org.mx
- Nueva Alianza.
  http://www.nuevaalianza-df.org.mx

Agrupaciones Políticas Locales

- Alianza de Organizaciones Sociales.
- Agrupación Cívica Democrática.
- Asociación Mexicana de la Familia “Pro Desarrollo Nacional”.
- Asociación Profesional Interdisciplinaria de México.
- Avance Ciudadano.
- Ciudadanos Activos del Distrito Federal.
- Ciudadanos Unidos por México.
- Comisión de Organizaciones del Transporte y Agrupaciones Ciudadanas.
- Comité de Defensa Popular del Valle de México.
- Conciencia Ciudadana.
- Coordinadora Ciudadana del Distrito Federal.
- Corriente Solidaridad.
- Esperanza Ciudadana.
- Frente del Pueblo.
- Fuerza Democrática.
- Fuerza del Tepeyac.
- Fuerza Nacionalista Mexicana.
- Fuerza Popular Línea de Masas.
- México Avanza.
- México Joven.
- Movimiento Civil 21.
- Movimiento Libertad.
- Movimiento Social Democrático.
- Mujeres Insurgentes.
- Organización Ciudadana en Beneficio del Distrito Federal.
- Organización Juvenil Participación Social Activa.
- Patria Nueva.
- Por la Tercera Vía.
- Proyecto Ciudadano.
- Proyecto Integral Democrático de Enlace (PIDE).
- Red Autogestionaria.
- Tiempo Democrático.
- Unidos por la Ciudad de México.
- Unión Ciudadana en Acción.
- Unión Nacional Interdisciplinaria de Ciudadanos en el Distrito Federal.
- Vida Digna.

Ley de Protección de Datos

Personales para el Distrito Federal (LPDPDF)

Publicada en la Gaceta Oficial del Distrito Federal el 3 de octubre de 2008

(Al margen superior un escudo que dice: Ciudad de México.- Capital en Movimiento)

DECRETO POR EL QUE SE EXPIDE LA LEY DE PROTECCIÓN DE DATOS PERSONALES PARA EL DISTRITO FEDERAL.

(Al margen superior un escudo que dice: Ciudad de México.- Capital en Movimiento)

DECRETO POR EL QUE SE EXPIDE LA LEY DE PROTECCIÓN DE DATOS PERSONALES PARA EL DISTRITO FEDERAL.

MARCELO LUIS EBRARD CASAUBON, Jefe de Gobierno del Distrito Federal, a sus habitantes sabed:

Que la H. Asamblea Legislativa del Distrito Federal, IV Legislatura se ha servido dirigirme el siguiente:

DECRETO

(Al margen superior izquierdo un sello con el Escudo Nacional que dice: ESTADOS UNIDOS MEXICANOS.- ASAMBLEA LEGISLATIVA DEL DISTRITO FEDERAL, IV LEGISLATURA)

ASAMBLEA LEGISLATIVA DEL DISTRITO FEDERAL

IV LEGISLATURA

D E C R E T A

DECRETO POR EL QUE SE EXPIDE LA LEY DE PROTECCIÓN DE DATOS PERSONALES PARA EL DISTRITO FEDERAL.

UNICO.- Se crea la Ley de Protección de Datos Personales para el Distrito Federal para quedar como sigue:

LEY DE PROTECCIÓN DE DATOS PERSONALES PARA EL DISTRITO FEDERAL

TÍTULO PRIMERO
DISPOSICIONES COMUNES PARA LOS ENTES PÚBLICOS

CAPÍTULO ÚNICO
DISPOSICIONES GENERALES

Artículo 1.- La presente Ley es de orden público e interés general y tiene por objeto establecer los principios, derechos, obligaciones y procedimientos que regulan la protección y tratamiento de los datos personales en posesión de los entes públicos.

Artículo 2.- Para los efectos de la presente Ley, se entiende por:

Bloqueo de datos personales: La identificación y reserva de datos personales con el fin de impedir su tratamiento;

Cesión de datos personales: Toda obtención de datos resultante de la consulta de un archivo, registro, base o banco de datos, una publicación de los datos contenidos en él, su interconexión con otros ficheros y la comunicación de datos realizada por una persona distinta a la interesada, así como la transferencia o comunicación de datos realizada entre entes públicos;

Datos personales: La información numérica, alfabética, gráfica, acústica o de cualquier otro tipo concerniente a una persona física, identificada o identificable. Tal y como son, de manera enunciativa y no

limitativa: el origen étnico o racial, características físicas, morales o emocionales, la vida afectiva y familiar, el domicilio y teléfono particular, correo electrónico no oficial, patrimonio, ideología y opiniones políticas, creencias, convicciones religiosas y filosóficas, estado de salud, preferencia sexual, la huella digital, el ADN y el número de seguridad social, y análogos;

Ente Público: La Asamblea Legislativa del Distrito Federal; el Tribunal Superior de Justicia del Distrito Federal; El Tribunal de lo Contencioso Administrativo del Distrito Federal; El Tribunal Electoral del Distrito Federal; el Instituto Electoral del Distrito Federal; la Comisión de Derechos Humanos del Distrito Federal; la Junta de Conciliación y Arbitraje del Distrito Federal; la Jefatura de Gobierno del Distrito Federal; las Dependencias, Órganos Desconcentrados, Órganos Político Administrativos y Entidades de la Administración Pública del Distrito Federal; los Órganos Autónomos por Ley; los partidos políticos, asociaciones y agrupaciones políticas; así como aquellos que la legislación local reconozca como de interés público y ejerzan gasto público; y los entes equivalentes a personas jurídicas de derecho público o privado, ya sea que en ejercicio de sus actividades actúen en auxilio de los órganos antes citados o ejerzan gasto público;

Instituto: El Instituto de Acceso a la Información Pública del Distrito Federal.

Interesado: Persona física titular de los datos personales que sean objeto del tratamiento al que se refiere la presente Ley;

Oficina de Información Pública: La unidad administrativa receptora de las solicitudes de acceso, rectificación, cancelación y oposición de datos personales en posesión de los entes públicos, a cuya tutela estará el trámite de las mismas, conforme a lo establecido en esta Ley y en los lineamientos que al efecto expida el Instituto;

Procedimiento de disociación. Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a una persona física identificada o identificable;

Responsable del Sistema de Datos Personales: Persona física que decida sobre la protección y tratamiento de datos personales, así como el contenido y finalidad de los mismos;

Sistema de Datos Personales: Todo conjunto organizado de archivos, registros, ficheros, bases o banco de datos personales de los entes públicos, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso;

Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos automatizados o físicos, aplicados a los sistemas de datos personales, relacionados con la obtención, registro, organización, conservación, elaboración, utilización, cesión, difusión, interconexión o cualquier otra forma que permita obtener información de los mismos y facilite al interesado el acceso, rectificación, cancelación u oposición de sus datos;

Usuario.- Aquel autorizado por el ente público para prestarle servicios para el tratamiento de datos personales.

Artículo 3.- La interpretación de esta ley se realizará conforme a la Constitución Política de los Estados Unidos Mexicanos, la Declaración Universal de los Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, la Convención Americana sobre Derechos Humanos, y demás instrumentos internacionales suscritos y ratificados por el Estado Mexicano y la interpretación que de los mismos hayan realizado los órganos internacionales respectivos.

Artículo 4.- En todo lo no previsto en los procedimientos a que se refiere esta Ley, se aplicará de manera supletoria la Ley de Procedimiento Administrativo del Distrito Federal y, en su defecto, el Código de Procedimientos Civiles del Distrito Federal.

TITULO SEGUNDO
DE LA TUTELA DE DATOS PERSONALES

CAPÍTULO I
DE LOS PRINCIPIOS

Artículo 5.- Los sistemas de datos personales en posesión de los entes públicos se regirán por los principios siguientes:

Licitud: Consiste en que la posesión y tratamiento de sistemas de datos personales obedecerá exclusivamente a las atribuciones legales o reglamentarias de cada ente público y deberán obtenerse a través de medios previstos en dichas disposiciones.

Los sistemas de datos personales no pueden tener finalidades contrarias a las leyes o a la moral pública y en ningún caso pueden ser utilizados para finalidades distintas o incompatibles con aquella que motivaron su obtención. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

Consentimiento: Se refiere a la manifestación de voluntad libre, inequívoca, específica e informada, mediante la cual el interesado consiente el tratamiento de sus datos personales.

Calidad de los Datos: Los datos personales recabados deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido. Los datos recabados deberán ser los que respondan con veracidad a la situación actual del interesado.

Confidencialidad: Consiste en garantizar que exclusivamente la persona interesada puede acceder a los datos personales o, en caso, el responsable o el usuario del sistema de datos personales para su tratamiento, así como el deber de secrecía del responsable del sistema de datos personales, así como de los usuarios.

Los instrumentos jurídicos que correspondan a la contratación de servicios del responsable del sistema de datos personales, así como de los usuarios, deberán prever la obligación de garantizar la seguridad y confidencialidad de los sistemas de datos personales, así como la prohibición de utilizarlos con propósitos distintos para los cuales se

llevó a cabo la contratación, así como las penas convencionales por su incumplimiento. Lo anterior, sin perjuicio de las responsabilidades previstas en otras disposiciones aplicables.

Los datos personales son irrenunciables, intransferibles e indelegables, por lo que no podrán transmitirse salvo disposición legal o cuando medie el consentimiento del titular y dicha obligación subsistirá aún después de finalizada la relación entre el ente público con el titular de los datos personales, así como después de finalizada la relación laboral entre el ente público y el responsable del sistema de datos personales o los usuarios.

El responsable del sistema de datos personales o los usuarios podrán ser relevados del deber de confidencialidad por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la seguridad nacional o la salud pública.

Seguridad: Consiste en garantizar que únicamente el responsable del sistema de datos personales o en su caso los usuarios autorizados puedan llevar a cabo el tratamiento de los datos personales, mediante los procedimientos que para tal efecto se establezcan.

Disponibilidad: Los datos deben ser almacenados de modo que permitan el ejercicio de los derechos de acceso, rectificación, cancelación y oposición del interesado.

Temporalidad: Los datos personales deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los que hubiesen sido recolectados.

Queda exceptuado el tratamiento que con posterioridad se les dé con objetivos estadísticos o científicos, siempre que cuenten con el procedimiento de disociación.

Únicamente podrán ser conservados de manera íntegra, permanente y sujetos a tratamiento los datos personales con fines históricos.

CAPÍTULO II
DE LOS SISTEMAS DE DATOS PERSONALES

Artículo 6.- Corresponde a cada ente público determinar, a través de su titular o, en su caso, del órgano competente, la creación, modificación o supresión de sistemas de datos personales, conforme a su respectivo ámbito de competencia.

Artículo 7.- La integración, tratamiento y tutela de los sistemas de datos personales se regirán por las disposiciones siguientes:

I. Cada ente público deberá publicar en la Gaceta Oficial del Distrito Federal la creación, modificación o supresión de su sistema de datos personales;

II. En caso de creación o modificación de sistemas de datos personales, se deberá indicar por lo menos:

a) La finalidad del sistema de datos personales y los usos previstos para el mismo;

b) Las personas o grupos de personas sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos;

c) El procedimiento de recolección de los datos de carácter personal;

d) La estructura básica del sistema de datos personales y la descripción de los tipos de datos incluidos en el mismo;

e) De la cesión de las que pueden ser objeto los datos;

f) Las instancias responsables del tratamiento del sistema de datos personales;

g) La unidad administrativa ante la que podrán ejercitarse los derechos de acceso, rectificación, cancelación u oposición; y

h) El nivel de protección exigible.

III. En las disposiciones que se dicten para la supresión de los sistemas de datos personales, se establecerá el destino de los datos contenidos en los mismos o, en su caso, las previsiones que se adopten para su destrucción.

IV. De la destrucción de los datos personales podrán ser excluidos aquellos que, con finalidades estadísticas o históricas, sean previamente sometidos al procedimiento de disociación.

Artículo 8.- Los sistemas de datos personales en posesión de los entes públicos deberán inscribirse en el registro que al efecto habilite el Instituto.

El registro debe comprender como mínimo la información siguiente:

I. Nombre y cargo del responsable y de los usuarios;

II. Finalidad del sistema;

III. Naturaleza de los datos personales contenidos en cada sistema;

IV. Forma de recolección y actualización de datos;

V. Destino de los datos y personas físicas o morales a las que pueden ser transmitidos;

VI. Modo de interrelacionar la información registrada;

VII. Tiempo de conservación de los datos, y

VIII. Medidas de seguridad.

Artículo 9.- Cuando los entes públicos recaben datos personales deberán informar previamente a los interesados de forma expresa, precisa e inequívoca lo siguiente:

I. De la existencia de un sistema de datos personales, del tratamiento de datos personales, de la finalidad de la obtención de éstos y de los destinatarios de la información;

II. Del carácter obligatorio o facultativo de responder a las preguntas que les sean planteadas;

III. De las consecuencias de la obtención de los datos personales, de la negativa a suministrarlos o de la inexactitud de los mismos;

IV. De la posibilidad para que estos datos sean difundidos, en cuyo caso deberá constar el consentimiento expreso del interesado, salvo cuando se trate de datos personales que por disposición de una Ley sean considerados públicos;

V. De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; y

VI. Del nombre del responsable del sistema de datos personales y en su caso de los destinatarios.

Cuando se utilicen cuestionarios u otros impresos para la obtención de los datos, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el presente artículo.

En caso de que los datos de carácter personal no hayan sido obtenidos del interesado, éste deberá ser informado de manera expresa, precisa e inequívoca, por el responsable del sistema de datos personales, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad de lo previsto en las fracciones I, IV y V del presente artículo.

Se exceptúa de lo previsto en el presente artículo cuando alguna ley expresamente así lo estipule.

Asimismo, tampoco regirá lo dispuesto en el presente artículo cuando los datos personales procedan de fuentes accesibles al público en general.

Artículo 10.- Ninguna persona está obligada a proporcionar datos personales considerados como sensibles, tal y como son: el origen étnico o racial, características morales o emocionales, ideología y opiniones políticas, creencias, convicciones religiosas, filosóficas y preferencia sexual.

Queda prohibida la creación de sistemas de datos personales que tengan la finalidad exclusiva de almacenar los datos personales señalados en el párrafo anterior y sólo pueden ser tratados cuando medien razones de interés general, así lo disponga una ley, lo consienta expresamente el interesado o, con fines estadísticos o históricos, siempre y cuando se hubiera realizado previamente el procedimiento de disociación.

Tratándose de estudios científicos o de salud pública el procedimiento de disociación no será necesario.

Artículo 11.- Los archivos o sistemas creados con fines administrativos por las dependencias, instituciones o cuerpos de seguridad pública, en los que se contengan datos de carácter personal, quedarán sujetos al régimen general de protección previsto en la presente Ley.

Los datos de carácter personal obtenidos para fines policiales, podrán ser recabados sin consentimiento de las personas a las que se refieren, pero estarán limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la prevención o persecución de delitos, debiendo ser almacenados en sistemas específicos, establecidos al efecto, que deberán clasificarse por categorías en función de su grado de confiabilidad.

La obtención y tratamiento de los datos a los que se refiere el presente artículo, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas por los interesados ante los órganos jurisdiccionales.

Los datos personales recabados con fines policiales se cancelarán cuando no sean necesarios para las investigaciones que motivaron su almacenamiento.

A estos efectos, se considerará especialmente la edad del interesado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.

Artículo 12.- Los responsables de los sistemas de datos personales con fines policiales, para la prevención de conductas delictivas o en materia tributaria, podrán negar el acceso, rectificación, oposición y cancelación de datos personales en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando, así como cuando los mismos obstaculicen la actuación de la autoridad durante el cumplimiento de sus atribuciones.

CAPÍTULO III
DE LAS MEDIDAS DE SEGURIDAD

Artículo 13.- Los entes públicos establecerán las medidas de seguridad técnica y organizativa para garantizar la confidencialidad e integralidad de cada sistema de datos personales que posean, con la finalidad de preservar el pleno ejercicio de los derechos tutelados en la presente Ley, frente a su alteración, pérdida, transmisión y acceso no autorizado, de conformidad al tipo de datos contenidos en dichos sistemas.

Dichas medidas serán adoptadas en relación con el menor o mayor grado de protección que ameriten los datos personales, deberán constar por escrito y ser comunicadas al Instituto para su registro.

Las medidas de seguridad que al efecto se establezcan deberán indicar el nombre y cargo del servidor público o, en su caso, la persona física o moral que intervengan en el tratamiento de datos personales con el carácter de responsable del sistema de datos personales o usuario, según corresponda. Cuando se trate de usuarios se deberán incluir los datos del acto jurídico mediante el cual, el ente público otorgó el tratamiento del sistema de datos personales.

En el supuesto de actualización de estos datos, la modificación respectiva deberá notificarse al Instituto, dentro de los 30 días hábiles siguientes a la fecha en que se efectuó.

Artículo 14.- El ente público responsable de la tutela y tratamiento del sistema de datos personales, adoptará las medidas de seguridad, conforme a lo siguiente:

A. Tipos de seguridad:

I. Física.- Se refiere a toda medida orientada a la protección de instalaciones, equipos, soportes o sistemas de datos para la prevención de riesgos por caso fortuito o causas de fuerza mayor;

II. Lógica.- Se refiere a las medidas de protección que permiten la identificación y autentificación de las personas o usuarios autorizados para el tratamiento de los datos personales de acuerdo con su función;

III. De desarrollo y aplicaciones.- Corresponde a las autorizaciones con las que deberá contar la creación o tratamiento de sistemas de datos

personales, según su importancia, para garantizar el adecuado desarrollo y uso de los datos, previendo la participación de usuarios, la separación de entornos, la metodología a seguir, ciclos de vida y gestión, así como las consideraciones especiales respecto de aplicaciones y pruebas;

IV. De cifrado.- Consiste en la implementación de algoritmos, claves, contraseñas, así como dispositivos concretos de protección que garanticen la integralidad y confidencialidad de la información; y

V. De comunicaciones y redes.- Se refiere a las restricciones preventivas y/o de riesgos que deberán observar los usuarios de datos o sistemas de datos personales para acceder a dominios o cargar programas autorizados, así como para el manejo de telecomunicaciones.

B. Niveles de seguridad:

I. Básico.- Se entenderá como tal, el relativo a las medidas generales de seguridad cuya aplicación es obligatoria para todos los sistemas de datos personales. Dichas medidas corresponden a los siguientes aspectos:

a) Documento de seguridad;

b) Funciones y obligaciones del personal que intervenga en el tratamiento de los sistemas de datos personales;

c) Registro de incidencias;

d) Identificación y autentificación;

e) Control de acceso;

f) Gestión de soportes, y

g) Copias de respaldo y recuperación.

II. Medio.- Se refiere a la adopción de medidas de seguridad cuya aplicación corresponde a aquellos sistemas de datos relativos a la comisión de infracciones administrativas o penales, hacienda pública, servicios financieros, datos patrimoniales, así como a los sistemas que contengan datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo. Este nivel de seguridad, de manera adicional a las medidas calificadas como básicas, considera los siguientes aspectos:

a) Responsable de seguridad;

b) Auditoría;

c) Control de acceso físico; y

d) Pruebas con datos reales.

III. Alto.- Corresponde a las medidas de seguridad aplicables a sistemas de datos concernientes a la ideología, religión, creencias, afiliación política, origen racial o étnico, salud, biométricos, genéticos o vida sexual, así como los que contengan datos recabados para fines policiales, de seguridad, prevención, investigación y persecución de delitos. Los sistemas de datos a los que corresponde adoptar el nivel de seguridad alto, además de incorporar las medidas de nivel básico y medio, deberán completar las que se detallan a continuación:

a) Distribución de soportes;

b) Registro de acceso; y

c) Telecomunicaciones.

Los diferentes niveles de seguridad serán establecidos atendiendo a las características propias de la información.

Artículo 15.- Las medidas de seguridad a las que se refiere el artículo anterior constituyen mínimos exigibles, por lo que el ente público adoptará las medidas adicionales que estime necesarias para brindar mayores garantías en la protección y resguardo de los sistemas de datos personales. Por la naturaleza de la información, las medidas de seguridad que se adopten serán consideradas confidenciales y únicamente se comunicará al Instituto, para su registro, el nivel de seguridad aplicable.

CAPÍTULO IV

DEL TRATAMIENTO DE DATOS PERSONALES

Artículo 16.- El tratamiento de los datos personales, requerirá el consentimiento inequívoco, expreso y por escrito del interesado, salvo en los casos y excepciones siguientes:

I. Cuando se recaben para el ejercicio de las atribuciones legales conferidas a los entes públicos;

II. Cuando exista una orden judicial;

III. Cuando se refieran a las partes de un convenio de una relación de negocios, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento;

IV. Cuando el interesado no esté en posibilidad de otorgar su consentimiento por motivos de salud y el tratamiento de sus datos resulte necesario para la prevención o para el diagnóstico médico, la prestación o gestión de asistencia sanitaria o tratamientos médicos, siempre que dicho tratamiento de datos se realice por una persona sujeta al secreto profesional u obligación equivalente;

V. Cuando la transmisión se encuentre expresamente prevista en una ley;

VI. Cuando la transmisión se produzca entre organismos gubernamentales y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos;

VII. Cuando se den a conocer a terceros para la prestación de un servicio que responda al tratamiento de datos personales, mediante la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente que la comunicación de los datos será legítima en cuanto se limite a la finalidad que la justifique;

VIII. Cuando se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia, o para la realización de estudios epidemiológicos; y

IX. Cuando los datos figuren en registros públicos en general y su tratamiento sea necesario siempre que no se vulneren los derechos y libertades fundamentales del interesado.

El consentimiento a que se refiere el presente artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.

El ente público no podrá difundir o ceder los datos personales contenidos en los sistemas de datos desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso por escrito o por un medio de autenticación similar, de las personas a que haga referencia la información. Al efecto, la oficina de información pública contará con los formatos necesarios para recabar dicho consentimiento.

El cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias del cedente, respondiendo solidariamente por la inobservancia de las mismas.

Artículo 17.- En los supuestos de utilización o cesión de los datos de carácter personal en que se impida gravemente o se atente de igual modo contra el ejercicio de derechos de las personas, el Instituto podrá requerir a los responsables de los sistemas de datos personales, la suspensión en la utilización o cesión de los datos. Si el requerimiento fuera desatendido, mediante resolución fundada y motivada, el Instituto podrá bloquear tales sistemas, de conformidad con el procedimiento que al efecto se establezca. El incumplimiento a la inmovilización ordenada por el Instituto será sancionado por la autoridad competente de conformidad por la Ley Federal de Responsabilidades de los Servidores Públicos.

Artículo 18.- El tratamiento de los sistemas de datos personales en materia de salud, se rige por lo dispuesto en la Ley General de Salud, la Ley de Salud para el Distrito Federal y demás normas que de ellas deriven. El tratamiento y cesión a esta información obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico asistencial, de manera tal que se mantenga la confidencialidad de los mismos, salvo que el propio paciente haya dado su consentimiento para no separarlos. Se exceptúan los supuestos de investigación científica, de salud pública o con fines judiciales, en los que se considere imprescindible la unificación de los datos identificativos con los clínico-asistenciales. El acceso a los datos y documentos relacionados con la salud de las personales queda limitado estrictamente a los fines específicos de cada caso.

Artículo 19.- Los sistemas de datos personales que hayan sido objeto de tratamiento, deberán ser suprimidos una vez que concluyan los plazos de conservación establecidos por las disposiciones aplicables, o cuando dejen de ser necesarios para los fines por los cuales fueron recabados.

En el caso de que el tratamiento de los sistemas haya sido realizado por una persona distinta al ente público, el instrumento jurídico que dio origen al mismo deberá establecer el plazo de conservación por el usuario, al término del cual los datos deberán ser devueltos en su totalidad al ente público, quien deberá garantizar su tutela o proceder, en su caso, a la supresión.

Artículo 20.- En caso de que los destinatarios de los datos sean instituciones de otras entidades federativas, los entes públicos deberán asegurarse que tales instituciones garanticen que cuentan con niveles de protección, semejantes o superiores, a los establecidos en esta Ley y, en la propia normatividad del ente público de que se trate.

En el supuesto de que los destinatarios de los datos sean personas o instituciones de otros países, el responsable del sistema de datos personales deberá realizar la cesión de los mismos, conforme a las disposiciones previstas en la legislación federal aplicable, siempre y cuando se garanticen los niveles de seguridad y protección previstos en la presente Ley.

CAPÍTULO V
DE LAS OBLIGACIONES DE LOS ENTES PÚBLICOS

Artículo 21.- El titular del ente público designará al responsable de los sistemas de datos personales, mismo que deberá:

I. Cumplir con las políticas y lineamientos así como las normas aplicables para el manejo, tratamiento, seguridad y protección de datos personales;

II. Adoptar las medidas de seguridad necesarias para la protección de datos personales y comunicarlas al Instituto para su registro, en los términos previstos en esta Ley;

III. Elaborar y presentar al Instituto un informe correspondiente sobre las obligaciones previstas en la presente Ley, a más tardar el último día hábil del mes de enero de cada año. La omisión de dicho informe será motivo de responsabilidad;

IV. Informar al interesado al momento de recabar sus datos personales, sobre la existencia y finalidad de los sistemas de datos personales,

así como el carácter obligatorio u optativo de proporcionarlos y las consecuencias de ello;

V. Adoptar los procedimientos adecuados para dar trámite a las solicitudes de informes, acceso, rectificación, cancelación y oposición de datos personales y, en su caso, para la cesión de los mismos; debiendo capacitar a los servidores públicos encargados de su atención y seguimiento;

VI. Utilizar los datos personales únicamente cuando éstos guarden relación con la finalidad para la cual se hayan obtenido;

VII. Permitir en todo momento al interesado el ejercicio del derecho de acceso a sus datos personales, a solicitar la rectificación o cancelación, así como a oponerse al tratamiento de los mismos en los términos de esta Ley;

VIII. Actualizar los datos personales cuando haya lugar, debiendo corregir o completar de oficio aquellos que fueren inexactos o incompletos, a efecto de que coincidan con los datos presentes del interesado, siempre y cuando se cuente con el documento que avale la actualización de dichos datos. Lo anterior, sin perjuicio del derecho del interesado para solicitar la rectificación o cancelación de los datos personales que le conciernen;

IX. Establecer los criterios específicos sobre el manejo, mantenimiento, seguridad y protección del sistema de datos personales;

X. Elaborar un plan de capacitación en materia de seguridad de datos personales;

XI. Resolver sobre el ejercicio de los derechos de acceso, rectificación, cancelación y oposición de los datos de las personas;

XII. Establecer los criterios específicos sobre el manejo, mantenimiento, seguridad y protección del sistema de datos personales;

XIII. Llevar a cabo o, en su caso, coordinar la ejecución material de las diferentes operaciones y procedimientos en que consista el tratamiento de datos y sistemas de datos de carácter personal a su cargo;

XIV. Coordinar y supervisar la adopción de las medidas de seguridad a que se encuentren sometidos los sistemas de datos personales de acuerdo con la normativa vigente;

XV. Dar cuenta de manera fundada y motivada a la autoridad competente de la aplicación de las excepciones al régimen general previsto para el acceso, rectificación, cancelación u oposición de datos personales; y

XVI. Las demás que se deriven de la presente Ley o demás ordenamientos jurídicos aplicables.

Artículo 22.- El titular del ente público será el responsable de decidir sobre la finalidad, contenido y uso del tratamiento del sistema de datos personales, quien podrá delegar dicha atribución en la unidad administrativa en la que se concrete la competencia material, a cuyo ejercicio sirva instrumentalmente el sistema de datos y esté adscrito el responsable del mismo.

TÍTULO TERCERO
DE LA AUTORIDAD RESPONSABLE DEL CONTROL Y VIGILANCIA

CAPÍTULO ÚNICO
DEL INSTITUTO Y SUS ATRIBUCIONES

Artículo 23.- El Instituto de Acceso a la Información Pública del Distrito Federal es el órgano encargado de dirigir y vigilar el cumplimiento de la presente Ley, así como de las normas que de ella deriven; será la autoridad encargada de garantizar la protección y el correcto tratamiento de datos personales.

Artículo 24.- El Instituto tendrá las atribuciones siguientes:

I. Establecer, en el ámbito de su competencia, políticas y lineamientos de observancia general para el manejo, tratamiento, seguridad y protección de los datos personales que estén en posesión de los entes públicos, así como expedir aquellas normas que resulten necesarias para el cumplimiento de esta Ley;

II. Diseñar y aprobar los formatos de solicitudes de acceso, rectificación, cancelación y oposición de datos personales;

III. Establecer sistemas electrónicos para la recepción y trámite de solicitudes de acceso, rectificación, cancelación y oposición de datos personales;

IV. Llevar a cabo el registro de los sistemas de datos personales en posesión de los entes públicos;

V. Elaborar y mantener actualizado el registro del nivel de seguridad aplicable a los sistemas de datos personales, en posesión de los entes públicos, en términos de esta Ley;

VI. Emitir opiniones sobre temas relacionados con la presente Ley, así como formular observaciones y recomendaciones a los entes públicos, derivadas del incumplimiento de los principios que rigen esta Ley;

VII. Hacer del conocimiento del órgano de control interno del ente público que corresponda, las resoluciones que emita relacionadas con la probable violación a las disposiciones materia de la presente Ley;

VIII. Orientar y asesorar a las personas que lo requieran acerca del contenido y alcance de la presente ley;

IX. Elaborar y publicar estudios e investigaciones para difundir el conocimiento de la presente Ley;

X. Solicitar y evaluar los informes presentados por los entes públicos respecto del ejercicio de los derechos previstos en esta Ley. Dicha evaluación se incluirá en el informe que de conformidad con el artículo 74 de la Ley de Transparencia y Acceso a la información pública presenta el Instituto a la Asamblea Legislativa del Distrito Federal y deberá incluir por lo menos:

a) El número de solicitudes de acceso, rectificación, cancelación y oposición de datos personales presentadas ante cada Ente Público, así como su resultado;

b). El tiempo de respuesta a la solicitud;

c). El estado que guardan las denuncias presentadas ante los órganos internos de control y las dificultades observadas en el cumplimiento de esta Ley;

d). El uso de los recursos públicos en la materia;

e). Las acciones desarrolladas;

f). Sus indicadores de gestión; y

g). El impacto de su actuación.

XI. Organizar seminarios, cursos, talleres y demás actividades que promuevan el conocimiento de la presente Ley y los derechos de las personas sobre sus datos personales;

XII. Establecer programas de capacitación en materia de protección de datos personales y promover acciones que faciliten a los entes públicos y a su personal participar de estas actividades, a fin de garantizar el adecuado cumplimiento de los principios que rigen la presente Ley;

XIII. Promover entre las instituciones educativas, públicas y privadas, la inclusión dentro de sus actividades académicas, curriculares y extracurriculares, los temas que ponderen la importancia del derecho a la protección de datos personales;

XIV. Promover la elaboración de guías que expliquen los procedimientos y trámites materia de esta Ley;

XV. Investigar, substanciar y resolver el recurso de revisión en los términos previstos en esta Ley y en la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal;

XVI. Evaluar la actuación de los Entes Públicos, mediante la práctica de visitas de inspección periódicas de oficio, a efecto de verificar la observancia de los principios contenidos en esta Ley, las cuales en ningún caso podrán referirse a información de acceso restringido de conformidad con la legislación aplicable;

XVII. Procurar la conciliación de los intereses de los interesados con los de los entes públicos, cuando éstos entren en conflicto con motivo de la aplicación de la presente Ley; y

XVIII. Las demás que establezca esta Ley, y demás ordenamientos aplicables.

Artículo 25.- A efecto de impulsar una cultura de protección de datos personales, se deberá promover el desarrollo de eventos que fomenten la profesionalización de los servidores públicos del Distrito Federal, sobre los sistemas y las medidas de seguridad que precisa la tutela de los datos personales de cada ente público.

TÍTULO CUARTO
DE LOS DERECHOS Y DEL PROCEDIMIENTO PARA SU EJERCICIO

CAPÍTULO I
DERECHOS EN MATERIA DE DATOS PERSONALES

Artículo 26.- Todas las personas, previa identificación mediante documento oficial, contarán con los derechos de acceso, rectificación, cancelación y oposición de sus datos personales en posesión de los entes públicos, siendo derechos independientes, de tal forma que no puede entenderse que el ejercicio de alguno de ellos sea requisito previo o impida el ejercicio de otro.

La respuesta a cualquiera de los derechos previstos en la presente ley, deberá ser proporcionada en forma legible e inteligible, pudiendo suministrase, a opción del interesado, por escrito o mediante consulta directa.

Artículo 27.- El derecho de acceso se ejercerá para solicitar y obtener información de los datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las cesiones realizadas o que se prevén hacer, en términos de lo dispuesto por esta Ley.

Artículo 28.- Procederá el derecho de rectificación de datos del interesado, en los sistemas de datos personales, cuando tales datos resulten inexactos o incompletos, inadecuados o excesivos, siempre y cuando no resulte imposible o exija esfuerzos desproporcionados.

No obstante, cuando se trate de datos que reflejen hechos constatados en un procedimiento administrativo o en un proceso judicial, aquellos se considerarán exactos siempre que coincidan con éstos.

Artículo 29.- El interesado tendrá derecho a solicitar la cancelación de sus datos cuando el tratamiento de los mismos no se ajuste a lo dispuesto en la Ley o en los lineamientos emitidos por el Instituto, o cuando hubiere ejercido el derecho de oposición y éste haya resultado procedente.

La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de los entes públicos, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el plazo deberá procederse a su supresión, en términos de la normatividad aplicable.

La supresión de datos no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando exista una obligación legal de conservar dichos datos.

Artículo 30.- El interesado tendrá derecho a oponerse al tratamiento de los datos que le conciernan, en el supuesto en que los datos se hubiesen recabado sin su consentimiento, cuando existan motivos fundados para ello y la ley no disponga lo contrario. De actualizarse tal supuesto, el responsable del sistema de datos personales deberá cancelar los datos relativos al interesado.

Artículo 31.- Si los datos rectificados o cancelados hubieran sido transmitidos previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan transmitido, en el caso de que se mantenga el tratamiento por este último, quién deberá también proceder a la rectificación o cancelación de los mismos.

CAPÍTULO II
DEL PROCEDIMIENTO

Artículo 32.- La recepción y trámite de las solicitudes de acceso, rectificación, cancelación u oposición de datos personales que se formule a los entes públicos se sujetarán al procedimiento establecido en el presente capítulo.

Sin perjuicio de lo que dispongan otras leyes, sólo el interesado o su representante legal, previa acreditación de su identidad, podrán solicitar al ente público, a través de la oficina de información pública competente, que le permita el acceso, rectificación, cancelación o haga efectivo su derecho de oposición, respecto de los datos personales que le conciernan y que obren en un sistema de datos personales en posesión del ente público.

La oficina de información pública del ente público deberá notificar al solicitante en el domicilio o medio electrónico señalado para tales efectos, en un plazo máximo de quince días hábiles contados desde la presentación de la solicitud, la determinación adoptada en relación con su solicitud, a efecto que, de resultar procedente, se haga efectiva la misma dentro de los diez días hábiles siguientes a la fecha de la citada notificación.

El plazo de quince días, referido en el párrafo anterior, podrá ser ampliado una única vez, por un periodo igual, siempre y cuando así lo justifiquen las circunstancias del caso.

Si al ser presentada la solicitud no es precisa o no contiene todos los datos requeridos, en ese momento el Ente Público, en caso de ser solicitud verbal, deberá ayudar al solicitante a subsanar las deficiencias. Si los detalles proporcionados por el solicitante no bastan para localizar los datos personales o son erróneos, la oficina de información pública del ente público podrá prevenir, por una sola vez y, dentro de los cinco días hábiles siguientes a la presentación de la solicitud, para que aclare o complete su solicitud, apercibido de que de no desahogar la prevención se tendrá por no presentada la solicitud.

Este requerimiento interrumpe los plazos establecidos en los dos párrafos anteriores.

En el supuesto que los datos personales a que se refiere la solicitud obren en los sistemas de datos personales del ente público y éste considere improcedente la solicitud de acceso, rectificación, cancelación u oposición, se deberá emitir una resolución fundada y motivada al respecto. Dicha respuesta deberá estar firmada por el titular de la oficina de información pública y por el responsable del sistema de datos personales del ente público.

Cuando los datos personales respecto de los cuales se ejerciten los derechos de acceso, rectificación, cancelación u oposición, no sean localizados en los sistemas de datos del ente público, se hará del conocimiento del interesado a través de acta circunstanciada, en la que se indiquen los sistemas de datos personales en los que se realizó la búsqueda. Dicha acta deberá estar firmada por un representante del órgano de control interno, el titular de la oficina de información pública y el responsable del sistema de datos personales del ente público.

Artículo 33.- La solicitud de acceso, rectificación, cancelación u oposición de datos personales, se deberá presentar ante la oficina de información pública del ente público que el interesado considere que está procesando información de su persona. El procedimiento de acceso, rectificación, cancelación u oposición de datos personales, iniciará con la presentación de una solicitud en cualquiera de las siguientes modalidades:

I. Por escrito material, será la presentada personalmente por el interesado o su representante legal, en la oficina de información pública, o bien, a través de correo ordinario, correo certificado o servicio de mensajería;

II. En forma verbal, será la que realiza el interesado o su representante legal directamente en la oficina de información pública, de manera oral y directa, la cual deberá ser capturada por el responsable de la oficina en el formato respectivo;

III. Por correo electrónico, será la que realiza el interesado a través de una dirección electrónica y sea enviada a la dirección de correo electrónico asignada a la oficina de información pública del ente público;

IV. Por el sistema electrónico que el Instituto establezca para tal efecto, y

V. Por vía telefónica, en términos de los lineamientos que expida el Instituto.

Artículo 34.- La solicitud de acceso, rectificación, cancelación u oposición de los datos personales deberá contener, cuando menos, los requisitos siguientes:

I. Nombre del ente público a quien se dirija;

II. Nombre completo del interesado, en su caso, el de su representante legal;

III. Descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos antes mencionados;

IV. Cualquier otro elemento que facilite su localización;

V. El domicilio, mismo que se debe encontrar dentro del Distrito Federal, o medio electrónico para recibir notificaciones, y

VI. Opcionalmente, la modalidad en la que prefiere se otorgue el acceso a sus datos personales, la cual podrá ser consulta directa, copias simples o certificadas.

En el caso de solicitudes de acceso a datos personales, el interesado, o en su caso, su representante legal deberá acreditar su identidad y personalidad al momento de la entrega de la información. Asimismo, deberá acreditarse la identidad antes de que el ente público proceda a la rectificación o cancelación.

En el caso de solicitudes de rectificación de datos personales, el interesado deberá indicar el dato que es erróneo y la corrección que debe realizarse y acompañar la documentación probatoria que sustente su petición, salvo que la misma dependa exclusivamente del consentimiento del interesado y ésta sea procedente.

En el caso de solicitudes de cancelación de datos personales, el interesado deberá señalar las razones por las cuales considera que el tratamiento de los datos no se ajusta a lo dispuesto en la Ley, o en su caso, acreditar la procedencia del ejercicio de su derecho de oposición.

Los medios por los cuales el solicitante podrá recibir notificaciones y acuerdos de trámite serán: correo electrónico, notificación personal en su domicilio o en la propia oficina de información pública que corresponda. En el caso de que el solicitante no señale domicilio o algún medio de los autorizados por esta ley para oír y recibir notificaciones, la prevención se notificará por lista que se fije en los estrados de la Oficina de Información Pública del Ente Público que corresponda.

El único medio por el cual el interesado podrá recibir la información referente a los datos personales será la oficina de información pública, y sin mayor formalidad que la de acreditar su identidad y cubrir los costos de conformidad con la presente Ley y el Código Financiero del Distrito Federal.

El Instituto y los entes públicos contarán con la infraestructura y los medios tecnológicos necesarios para garantizar el efectivo acceso a la información de las personas con discapacidad.

Artículo 35.- Presentada la solicitud de acceso, rectificación, cancelación u oposición de datos personales, la oficina de información pública del ente público, observará el siguiente procedimiento:

I. Procederá a la recepción y registro de la solicitud y devolverá al interesado, una copia de la solicitud registrada, que servirá de acuse de recibo, en la que deberá aparecer sello institucional, la hora y la fecha del registro;

II. Registrada la solicitud, se verificará si cumple con los requisitos establecidos por el artículo anterior, de no ser así se prevendrá al interesado, tal y como lo señala el artículo 32 de la presente Ley. De cumplir con los requisitos se turnará a la unidad administrativa que corresponda para que proceda a la localización de la información solicitada, a fin de emitir la respuesta que corresponda;

III. La unidad administrativa informará a la oficina de información pública de la existencia de la información solicitada. En caso de inexistencia, se procederá de conformidad con lo previsto por el artículo 32 para que la oficina de información pública a su vez realice una nueva búsqueda en otra área o unidad administrativa.

En la respuesta, la oficina de información pública, señalará el costo que por concepto de reproducción deberá pagar el solicitante en los términos del Código Financiero del Distrito Federal;

IV. La oficina de información pública, notificará en el domicilio o a través del medio señalado para tal efecto, la existencia de una respuesta para que el interesado o su representante legal pasen a recogerla a la oficina de información pública;

V. En cualquier caso, la entrega en soporte impreso o el acceso electrónico directo a la información solicitada se realizará de forma personal al interesado o a su representante legal; y

VI. Previa exhibición del original del documento con el que acreditó su identidad el interesado o su representante legal, se hará entrega de la información requerida.

En caso de que el ente público determine que es procedente la rectificación o cancelación de los datos personales, deberá notificar al interesado la procedencia de su petición, para que, dentro de los 10 días hábiles siguientes, el interesado o su representante legal acrediten

fehacientemente su identidad ante la oficina de información pública y se proceda a la rectificación o cancelación de los datos personales.

Artículo 36.- En caso de que no proceda la solicitud, la oficina de información pública deberá notificar al peticionario de manera fundada y motivada las razones por las cuales no procedió su petición. La respuesta deberá estar firmada por el titular de la oficina de información pública y por el responsable del sistema de datos personales, pudiendo recaer dichas funciones en la misma persona.

Artículo 37.- El trámite de solicitud de acceso, rectificación, cancelación u oposición de datos de carácter personal es gratuito. No obstante, el interesado deberá cubrir los costos de reproducción de los datos solicitados, en términos de lo previsto por el Código Financiero del Distrito Federal.

Los costos de reproducción de la información solicitada se cobrarán al solicitante de manera previa a su entrega y se calculará atendiendo a:

I. El costo de los materiales utilizados en la reproducción de la información;

II. El costo de envío; y

III. La certificación de documentos cuando proceda.

Los Entes Públicos deberán esforzarse por reducir al máximo, los costos de entrega de información.

CAPÍTULO III
DEL RECURSO DE REVISIÓN

Artículo 38.- Podrá interponer recurso de revisión ante el Instituto, el interesado que se considere agraviado por la resolución definitiva, que recaiga a su solicitud de acceso, rectificación, cancelación u oposición o ante la omisión de la respuesta. Para este efecto, las oficinas de información pública al dar respuesta a las solicitudes, orientarán al particular sobre su derecho de interponer el recurso de revisión y el modo y plazo para hacerlo.

Lo anterior, sin perjuicio del derecho que les asiste a los interesados de interponer queja ante los órganos de control interno de los entes obligados.

Artículo 39.- El Instituto tendrá acceso a la información contenida en los sistemas de datos personales que resulte indispensable para resolver el recurso. Dicha información deberá ser mantenida con carácter confidencial y no estará disponible en el expediente.

Las resoluciones que emita el Instituto serán definitivas, inatacables y obligatorias para los entes públicos y los particulares.

En contra de las resoluciones del Instituto el particular podrá interponer juicio de amparo.

La autoridad judicial competente tendrá acceso a los sistemas de datos personales cuando resulte indispensable para resolver el asunto y hubiera sido ofrecida en juicio. Dicha información deberá ser mantenida con ese carácter y no estará disponible en el expediente.

Artículo 40.- El recurso de revisión será tramitado de conformidad con los términos, plazos y requisitos señalados en la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal.

Igualmente, el recurrente podrá interponer el recurso de revocación, que será sustanciado en los términos que establezca la propia Ley de Transparencia y Acceso a la Información Pública del Distrito Federal y el Reglamento Interior del Instituto.

TÍTULO QUINTO
DE LAS RESPONSABILIDADES

CAPÍTULO ÚNICO
DE LAS INFRACCIÓNES

Artículo 41.- Constituyen infracciones a la presente Ley:

I. La omisión o irregularidad en la atención de solicitudes de acceso, rectificación, cancelación u oposición de datos personales;

II. Impedir, obstaculizar o negar el ejercicio de derechos a que se refiere la presente Ley;

III. Recabar datos de carácter personal sin proporcionar la información prevista en la presente Ley;

IV. Crear sistema de datos de carácter personal, sin la publicación previa en la Gaceta Oficial del Distrito Federal;

V. Obtener datos sin el consentimiento expreso del interesado cuando éste es requerido;

VI. Incumplir los principios previstos por la presente Ley;

VII. Transgredir las medidas de protección y confidencialidad a las que se refiere la presente Ley;

VIII. Omitir total o parcialmente el cumplimiento de las resoluciones realizadas por el Instituto, así como obstruir las funciones del mismo;

IX. Omitir o presentar de manera extemporánea los informes a que se refiere la presente Ley;

X. Obtener datos personales de manera engañosa o fraudulenta;

XI. Transmitir datos personales, fuera de los casos permitidos, particularmente cuando la transmisión haya tenido por objeto obtener un lucro indebido;

XII. Impedir u obstaculizar la inspección ordenada por el Instituto o su instrucción de bloqueo de sistemas de datos personales, y

XIII. Destruir, alterar, ceder datos personales, archivos o sistemas de datos personales sin autorización;

XIV. Incumplir con la inmovilización de sistemas de datos personales ordenada por el Instituto, y

XV. El incumplimiento de cualquiera de las disposiciones contenidas en esta Ley.

Las infracciones a que se refiere este artículo o cualquiera otra derivada del incumplimiento de las obligaciones establecidas en esta Ley, será sancionada en términos de la Ley de Federal de Responsabilidades de los Servidores Públicos, siendo independientes de las de orden civil o penal que procedan, así como los procedimientos para el resarcimiento del daño ocasionado por el ente público.

Artículo 42.- El Instituto denunciará ante las autoridades competentes cualquier conducta prevista en el artículo anterior y aportará las pruebas que considere pertinentes. Los órganos de control y fiscalización internos de los entes públicos entregarán semestralmente al Instituto, un informe estadístico de los procedimientos administrativos iniciados con motivo del incumplimiento de la presente Ley y sus resultados.

Esta información será incorporada al informe anual del Instituto.

Dicha resolución se comunicará al Ente Público y al responsable del sistema de datos personales y, en su caso, a los interesados de los datos personales que resultaren afectados.

Lo anterior sin perjuicio de las responsabilidades penales o civiles que pudieran derivarse.

TRANSITORIOS

PRIMERO.- El presente decreto entrará en vigor al día siguiente de su publicación en la Gaceta Oficial del Distrito Federal. Publíquese en el Diario de la Federación para su mayor difusión.

SEGUNDO.- Publíquese en la Gaceta Oficial del Distrito Federal para su debida observancia y aplicación.

TERCERO.- Los entes públicos deberán notificar al Instituto, treinta días hábiles después de la entrada en vigor de la presente Ley, la relación de Sistemas de Datos Personales que posean para su registro.

CUARTO.- El documento en el que se establezcan los niveles de seguridad a las que se refiere el capítulo III del Título II de la presente Ley, deberá ser emitido por los entes públicos dentro de los sesenta días hábiles posteriores a la entrada en vigor de la Ley, mismo que deberá ser remitido al Instituto para su registro dentro del mismo plazo.

Recinto de la Asamblea Legislativa del Distrito Federal, a los veintisiete días del mes de agosto del año dos mil ocho.-POR LA MESA DIRECTIVA.- DIP. AGUSTÍN CARLOS CASTILLA MARROQUÍN, PRESIDENTE

SECRETARIA, DIP. LETICIA QUEZADA CONTRERAS.- SECRETARIO, DIP. ALFREDO VINALAY MORA.-FIRMAS.

En cumplimiento de lo dispuesto por los artículos 122, apartado C, Base Segunda, fracción II, inciso b), de la Constitución Política de los Estados Unidos Mexicanos; 48, 49 y 67, fracción II, del Estatuto de Gobierno del Distrito Federal, para su debida publicación y observancia, expido el presente Decreto Promulgatorio, en la Residencia Oficial del Jefe de Gobierno del Distrito Federal, en la Ciudad de México, a los dieciocho días del mes de septiembre del año dos mil ocho.- JEFE DE GOBIERNO DEL DISTRITO FEDERAL, MARCELO LUIS EBRARD CASAUBON.- FIRMA.- SECRETARIO DE GOBIERNO, JOSÉ ÁNGEL ÁVILA PÉREZ.- FIRMA.- SECRETARIO DE DESARROLLO URBANO Y VIVIENDA, JESÚS ARTURO AISPURO CORONEL.- FIRMA.- SECRETARIA DE DESARROLLO ECONÓMICO, LAURA VELÁSQUEZ ALZÚA.- FIRMA.- SECRETARIA DEL MEDIO AMBIENTE, MARTHA TERESA DELGADO PERALTA.- FIRMA.- SECRETARIO DE OBRAS Y SERVICIOS, JORGE ARGANIS DÍAZ LEAL.- FIRMA.- SECRETARIO DE DESARROLLO SOCIAL, MARTÍ BATRES GUADARRAMA.- FIRMA.-SECRETARIO DE SALUD, DR. ARMANDO AHUE ORTEGA.- FIRMA.- SECRETARIO DE FINANZAS, LIC. MARIO MARTÍN DELGADO CARRILLO.- FIRMA.- SECRETARIO DE TRANSPORTES Y VIALIDAD, ARMANDO QUINTERO MARTÍNEZ.- FIRMA.- SECRETARIO DE SEGURIDAD PÚBLICA, MANUEL MONDRAGÓN Y KALB.- FIRMA.- SECRETARIO DE TURISMO, ALEJANDRO ROJAS DÍAZ DURÁN.-FIRMA.- SECRETARIA DE CULTURA, ELENA CEPEDA DE LEÓN.- FIRMA.- SECRETARIO DE PROTECCIÓN CIVIL, ELÍAS MIGUEL MORENO BRIZUELA.- FIRMA.- SECRETARIO DE TRABAJO Y FOMENTO AL EMPLEO, BENITO MIRÓN LINCE.- FIRMA.- SECRETARIO DE EDUCACIÓN, AXEL DIDRIKSSON TAKAYANAGUI.- FIRMA.- SECRETARIA DE DESARROLLO RURAL Y EQUIDAD PARA LAS COMUNIDADES, MARÍA ROSA MÁRQUEZ CABRERA.- FIRMA.

Lineamientos para la Protección de Datos Personales en el Distrito Federal

TÍTULO PRIMERO. DISPOSICIONES COMUNES PARA LOS ENTES PÚBLICOS

CAPÍTULO ÚNICO. DISPOSICIONES GENERALES

Objeto

1. Los presentes Lineamientos son de observancia obligatoria para los entes públicos y tienen por objeto establecer las directrices y criterios para la aplicación e implementación de la Ley de Protección de Datos Personales para el Distrito Federal.

Interpretación

2. La interpretación de estos Lineamientos se realizará conforme a lo dispuesto por el artículo 3 de la Ley de Protección de Datos Personales para el Distrito Federal.

Definiciones

3. Para los efectos de la Ley de Protección de Datos Personales para el Distrito Federal y de los presentes Lineamientos, además de las definiciones contenidas en la propia Ley, se entenderá por:

Autentificación: Comprobación de la identidad de aquella persona autorizada para el tratamiento de datos personales;

Bloqueo: Identificación y conservación de datos personales con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo, legal o contractual, de prescripción de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación del sistema a que correspondan;

Cancelación: Eliminación de determinados datos de un sistema de datos personales previo bloqueo de los mismos;

Cesionario: Persona física o moral, pública o privada, a la que un ente público realice una cesión de datos personales;

Documentos: Los expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares,

contratos, convenios, instructivos, notas, memorandos, estadísticas, o bien cualquier otro registro en posesión de los entes públicos sin importar su fuente o fecha de elaboración. Los documentos podrán estar en cualquier soporte, demás análogos escrito, impreso, sonoro, visual, electrónico, informático u holográfico;

Documento de seguridad: Instrumento que establece las medidas y procedimientos administrativos, físicos y técnicos de seguridad aplicables a los sistemas de datos personales necesarios para garantizar la protección, confidencialidad, integridad y disponibilidad de los datos contenidos en dichos sistemas;

Encargado: Servidor público que en ejercicio de sus atribuciones, realiza tratamiento de datos personales de forma cotidiana;

Enlace: Servidor público que fungirá como vínculo entre el ente público y el Instituto para atender los asuntos relativos a la Ley de la materia;

Fuente de acceso público: Aquella cuya consulta pueda ser realizada por cualquier persona, no impedida por una norma limitativa, sin más exigencia que, en su caso, el pago que genere el acceso a determinado medio de información. Tendrán el carácter de fuentes de acceso público los Registros Públicos, los diarios, gacetas y boletines gubernamentales, así como otros medios oficiales de difusión;

Incidencia: Cualquier anomalía que afecte o pudiera afectar la seguridad de los datos personales;

INFOMEX: Sistema electrónico mediante el cual las personas podrán presentar sus solicitudes de acceso a la información pública y de acceso, rectificación, cancelación y oposición de datos personales y es el sistema único para el registro y captura de todas las solicitudes recibidas por los entes públicos a través de los medios señalados en la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal y la Ley de Protección de Datos Personales para el Distrito Federal, así como para la recepción de los recursos de revisión interpuestos a través del propio sistema;

Inmovilización: Medida cautelar que consiste en la interrupción temporal en el uso de un sistema de datos personales ordenada por el Instituto en los supuestos de tratamiento ilícito de datos de carácter personal;

Lineamientos: Lineamientos para la Protección de Datos Personales en el Distrito Federal;

Ley: Ley de Protección de Datos Personales para el Distrito Federal;

Registro Electrónico de Sistemas de Datos Personales: Aplicación informática desarrollada por el Instituto para la inscripción de los sistemas de datos personales en posesión de los entes públicos;

Responsable: El servidor público de la unidad administrativa a la que se encuentre adscrito el sistema de datos personales, designado por el titular del ente público, que decide sobre el tratamiento de datos personales, así como el contenido y finalidad de los sistemas de datos personales;

Responsable de seguridad: persona a la que el responsable del sistema de datos personales asigna formalmente la función de coordinar y controlar las medidas de seguridad aplicables;

Sistema de Datos Personales: Conjunto organizado de datos personales que estén en posesión de los entes públicos, contenidos en archivos, registros, ficheros, bases o bancos de datos, que permita el acceso a datos con arreglo a criterios determinados, cualquiera que fuere la modalidad de su creación, almacenamiento, organización o acceso;

Soporte físico: Son los medios de almacenamiento inteligibles a simple vista, es decir, que no requieren de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos; es decir, documentos, oficios, formularios impresos llenados “a mano” o “a máquina”, fotografías, placas radiológicas, carpetas, expedientes, demás análogos;

Soporte electrónico: Son los medios de almacenamiento inteligibles sólo mediante el uso de algún aparato con circuitos electrónicos que procese su contenido para examinar, modificar o almacenar los datos; es decir, cintas magnéticas de audio, vídeo y datos, fichas de microfilm, discos ópticos (CDs y DVDs), discos magneto-ópticos, discos magnéticos (flexibles y duros) y demás medios de almacenamiento masivo no volátil;

Supresión: Eliminación de un sistema de datos personales mediante acuerdo publicado en la Gaceta Oficial del Distrito Federal; y

Suspensión: Medida cautelar ordenada por el Instituto que consiste en la interrupción temporal en el tratamiento de determinados datos personales contenidos en un sistema de datos personales.

TÍTULO SEGUNDO. DE LA TUTELA DE DATOS PERSONALES

CAPÍTULO I. DE LOS SISTEMAS DE DATOS PERSONALES

Tipos de sistemas de datos personales

4. Los sistemas de datos personales se distinguen en:

Físicos: Conjunto ordenado de datos de carácter personal que para su tratamiento están contenidos en registros manuales, impresos, sonoros, magnéticos, visuales u holográficos, estructurado conforme a criterios específicos relativos a personas físicas que permitan acceder sin esfuerzos desproporcionados a sus datos personales; y

Automatizados: Conjunto ordenado de datos de carácter personal que permita acceder a la información relativa a una persona física utilizado una herramienta tecnológica.

Categorías de datos personales

5. Los datos personales contenidos en los sistemas se clasificarán, de manera enunciativa, más no limitativa, de acuerdo a las siguientes categorías:

Datos identificativos: El nombre, domicilio, teléfono particular, teléfono celular, firma, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), Matrícula del Servicio Militar Nacional, número de pasaporte, lugar y fecha de nacimiento, nacionalidad, edad, fotografía, demás análogos;

Datos electrónicos: Las direcciones electrónicas, tales como, el correo electrónico no oficial, dirección IP (Protocolo de Internet), dirección MAC (dirección Media Access Control o dirección de control de acceso al medio), así como el nombre del usuario, contraseñas, firma electrónica; o cualquier otra información empleada por la persona, para su identificación en Internet u otra red de comunicaciones electrónicas;

Datos laborales: Documentos de reclutamiento y selección, nombramiento, incidencia, capacitación, actividades extracurriculares, referencias laborales, referencias personales, solicitud de empleo, hoja de servicio, demás análogos;

Datos patrimoniales: Los correspondientes a bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, fianzas, servicios contratados, referencias personales, demás análogos;

Datos sobre procedimientos administrativos y/o jurisdiccionales: La información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal, fiscal, administrativa o de cualquier otra rama del Derecho;

Datos académicos: Trayectoria educativa, calificaciones, títulos, cédula profesional, certificados y reconocimientos, demás análogos;

Datos de tránsito y movimientos migratorios: Información relativa al tránsito de las personas dentro y fuera del país, así como información migratoria;

Datos sobre la salud: El expediente clínico de cualquier atención médica, referencias o descripción de sintomatologías, detección de enfermedades, incapacidades médicas, discapacidades, intervenciones quirúrgicas, vacunas, consumo de estupefacientes, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, así como el estado físico o mental de la persona;

Datos biométricos: huellas dactilares, ADN, geometría de la mano, características de iris y retina, demás análogos;

Datos especialmente protegidos (sensibles): origen étnico o racial, características morales o emocionales, ideología y opiniones políticas, creencias, convicciones religiosas, filosóficas y preferencia sexual; y

Datos personales de naturaleza pública: aquellos que por mandato legal sean accesibles al público.

Creación, modificación o supresión de sistemas de datos personales

6. La creación, modificación o supresión de sistemas de datos personales de los entes públicos sólo podrá efectuarse mediante acuerdo emitido por el titular del ente o, en su caso, del órgano competente, publicado en la Gaceta Oficial del Distrito Federal.

En los casos de creación y modificación el acuerdo deberá dictarse y publicarse con, al menos quince días hábiles previos a la creación o modificación del sistema correspondiente.

Contenido del acuerdo de creación de un sistema de datos personales

7. El acuerdo de creación de sistemas de datos personales deberá contener:

La identificación del sistema de datos personales, indicando su denominación y normativa aplicable, así como la descripción de la finalidad y usos previstos;

El origen de los datos, indicando el colectivo de personas sobre las que se pretende obtener datos de carácter personal, o que resulten obligados a suministrarlos; su procedencia (propio interesado, representante, ente público, etcétera) así como el procedimiento de obtención de los mismos (formulario, Internet, transmisión electrónica, etcétera);

La estructura básica del sistema de datos personales mediante la descripción detallada de los datos identificativos que contiene y, en su caso, de los datos especialmente protegidos, así como las restantes categorías de datos de carácter personal, incluidas en el mismo y el modo de tratamiento utilizado en su organización (manual o automatizado). En su caso, señalar los datos de carácter obligatorio y facultativo;

Las cesiones de datos que se tengan previstas, indicando, en su caso, los destinatarios o categorías de destinatarios;

La identificación de la unidad administrativa a la que corresponde el sistema de datos personales, así como del cargo del responsable;

Domicilio oficial y dirección electrónica de la Oficina de Información Pública ante la cual se presentarán las solicitudes para ejercer los

derechos de acceso, rectificación, cancelación y oposición, así como la revocación del consentimiento; e

Indicación del nivel de seguridad que resulte aplicable: básico, medio o alto.

Modificación de sistemas de datos personales

8. El acuerdo mediante el cual se determine la modificación de un sistema de datos personales deberá indicar las modificaciones producidas en cualquiera de las fracciones a que se hace referencia en el numeral 7 de estos Lineamientos.

Todo acuerdo de modificación que afecte la integración y tratamiento de un sistema de datos personales debe publicarse en la Gaceta Oficial del Distrito Federal y ser notificado al Instituto dentro de los diez días hábiles siguientes a su publicación.

Dicha modificación también deberá ser inscrita por el responsable en el Registro Electrónico de Sistemas de Datos Personales, dentro del mismo plazo.

Supresión de sistemas de datos personales

9. En caso de que el titular del ente público o, en su caso, el responsable del sistema de datos personales determine la supresión de un sistema de datos personales mediante la publicación del acuerdo respectivo en la Gaceta Oficial del Distrito Federal, la supresión deberá ser notificada al Instituto dentro de los diez días hábiles siguientes, a efecto de que se proceda a la cancelación de inscripción en el registro correspondiente.

En los acuerdos que se emitan para la supresión de sistemas de datos personales se establecerá el destino que vaya a darse a los datos contenidos en los mismos o, en su caso, las previsiones que se adopten para su destrucción, de conformidad con la Ley de Archivos del Distrito Federal y demás normativa que resulte aplicable.

Asimismo, la publicación de estos acuerdos en la Gaceta Oficial del Distrito Federal deberá ser, al menos, treinta días hábiles previos a la supresión del sistema de que se trate.

No procederá la supresión de los sistemas de datos personales cuando exista una previsión expresa en una Ley que exija su conservación.

Registro de sistemas de datos personales

10. Los responsables de los sistemas de datos personales en posesión de los entes públicos deberán inscribir dichos sistemas en el Registro Electrónico de Sistemas de Datos Personales habilitado por el Instituto, en un plazo no mayor a los 10 días hábiles siguientes a la publicación de su creación en la Gaceta Oficial del Distrito Federal.

Contenido del Registro

11. El registro de cada sistema contendrá los siguientes campos:

Nombre del Sistema y, en su caso, fecha de publicación en la Gaceta Oficial del Distrito Federal;

Nombre y cargo del responsable del sistema;

Finalidades y usos previstos, así como el soporte en el que se encuentra;

La categoría de los datos personales contenidos en el sistema, forma de recolección y actualización de los mismos;

Unidad administrativa en la que se encuentra el sistema;

Destino y personas físicas o morales a las que puedan ser transmitidos;

Modo de interrelacionar la información contenida en el sistema y el plazo de conservación de los datos;

Teléfono y correo electrónico del responsable;

Normativa aplicable al sistema; e

Indicación del nivel de seguridad aplicable: básico, medio o alto.

El Instituto otorgará al Responsable un folio de identificación por cada sistema de datos personales inscrito.

Deber de información

12. A efecto de cumplir con el deber de información previsto en el artículo 9 de la Ley, en el momento en que se recaben datos personales,

por cualquier medio, el ente público deberá hacer del conocimiento del interesado las advertencias a las que se refiere dicho artículo.

Modelo de leyenda

13. Sin perjuicio de la modalidad mediante la cual los entes públicos recaben datos personales, éstos, deberán utilizar el siguiente modelo de leyenda para informar al interesado de las advertencias a que se refiere el artículo 9 de la Ley:

"Los datos personales recabados serán protegidos, incorporados y tratados en el Sistema de Datos Personales (nombre del sistema de datos personales), el cual tiene su fundamento en (fundamento legal que faculta al Ente público para recabar los datos personales), cuya finalidad es (describir la finalidad del sistema) y podrán ser transmitidos a (destinatario y finalidad de la transmisión), además de otras transmisiones previstas en la Ley de Protección de Datos Personales para el Distrito Federal.

Los datos marcados con un asterisco (*) son obligatorios y sin ellos no podrá acceder al servicio o completar el trámite (indicar el servicio o trámite de que se trate)

Asimismo, se le informa que sus datos no podrán ser difundidos sin su consentimiento expreso, salvo las excepciones previstas en la Ley.

El responsable del Sistema de datos personales es (nombre del responsable), y la dirección donde podrá ejercer los derechos de acceso, rectificación, cancelación y oposición, así como la revocación del consentimiento es (indicar el domicilio de la Oficina de Información Pública correspondiente).

El interesado podrá dirigirse al Instituto de Acceso a la Información Pública del Distrito Federal, donde recibirá asesoría sobre los derechos que tutela la Ley de Protección de Datos Personales para el Distrito Federal al teléfono: 5636-4636; correo electrónico: datos.personales@infodf.org.mx o www.infodf.org.mx"

Excepciones al deber de información

14. En el caso de datos personales que no hayan sido obtenidos directamente del interesado, no habrá obligación de cumplir con el de-

ber de información cuando resulte material o jurídicamente imposible o requiera de esfuerzos desproporcionados, en razón del número de interesados y/o la antigüedad de los datos.

CAPÍTULO II. DE LAS MEDIDAS DE SEGURIDAD

15. Las medidas de seguridad aplicables a los sistemas de datos personales responderán a los niveles establecidos en la Ley para cada tipo de datos. Dichas medidas deberán tomar en consideración las recomendaciones, que en su caso, emita el Instituto para este fin, con el objeto de garantizar la confidencialidad, integridad y disponibilidad de los datos personales durante su tratamiento.

Niveles de seguridad

16. Las medidas de seguridad se clasifican, en términos del artículo 14 de la Ley, en tres niveles: básico, medio y alto. Estas medidas son acumulativas y atenderán a lo siguiente:

I. Nivel Básico. El nivel de seguridad básico es aplicable a todos los sistemas de datos personales y comprende los siguientes aspectos:

a) Documento de seguridad:

El responsable elaborará, difundirá e implementará la normativa de seguridad mediante el documento de seguridad que será de observancia obligatoria para todos los servidores públicos del ente público, así como para toda aquella persona que debido a la prestación de un servicio tenga acceso a los sistemas de datos personales y/o al sitio donde se ubican los mismos, tomando en cuenta lo dispuesto en la Ley y en los presentes Lineamientos.

El documento de seguridad deberá contener, como mínimo, los siguientes aspectos:

Nombre del sistema;

Cargo y adscripción del responsable;

Ámbito de aplicación;

Estructura y descripción del sistema de datos personales;

Especificación detallada de la categoría de datos personales contenidos en el sistema;

Funciones y obligaciones del personal que intervenga en el tratamiento de los sistemas de datos personales;

Medidas, normas, procedimientos y criterios enfocados a garantizar el nivel de seguridad exigido por el artículo 14 de la Ley y los presentes Lineamientos;

Procedimientos de notificación, gestión y respuesta ante incidencias;

Procedimientos para la realización de copias de respaldo y recuperación de los datos, para los sistemas de datos personales automatizados; y

Procedimientos para la realización de auditorías, en su caso.

El documento de seguridad deberá actualizarse anualmente o cuando se produzcan cambios relevantes en el tratamiento, que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas.

b) Funciones y obligaciones del responsable, encargado y de toda persona que intervenga en el tratamiento de los sistemas de datos personales:

Las funciones y obligaciones de todos los que intervengan en el tratamiento de datos personales deben estar claramente definidas en el documento de seguridad. El responsable adoptará las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones, así como las responsabilidades y consecuencias en que pudiera incurrir en caso de incumplimiento.

c) Registro de incidencias:

Los procedimientos de notificación gestión y respuesta ante incidencias contarán necesariamente con un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las acciones implementadas.

d) Identificación y autentificación:

El responsable tendrá a su cargo la elaboración de una relación actualizada de servidores públicos que tengan acceso autorizado al sistema de datos personales y de establecer procedimientos que permitan la correcta identificación y autenticación para dicho acceso.

El responsable establecerá un mecanismo que permita la identificación, de forma inequívoca y personalizada, de toda aquella persona que intente acceder al sistema de datos personales y la verificación de que está autorizada.

Cuando el mecanismo de autenticación se base en la existencia de contraseñas se establecerá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

Las contraseñas se cambiarán con la periodicidad que se determine en el documento de seguridad y se conservarán cifradas. Asimismo, se establecerá un procedimiento de creación y modificación de contraseñas (longitud, formato, contenido).

e) Control de acceso:

El responsable deberá adoptar medidas para que los encargados y usuarios tengan acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.

El responsable deberá mantener actualizada una relación de personas autorizadas y los accesos autorizados para cada una de ellas. Asimismo, deberá establecer los procedimientos para el uso de bitácoras respecto de las acciones cotidianas llevadas a cabo en el sistema de datos personales.

Solamente el responsable podrá conceder, alterar o anular la autorización para el acceso a los sistemas de datos personales.

f) Gestión de soportes:

Al almacenar los soportes físicos y electrónicos que contengan datos de carácter personal se deberá cuidar que estén etiquetados para permitir identificar el tipo de información que contienen, ser inventariados

y sólo podrán ser accesibles por el personal autorizado para ello en el documento de seguridad.

La salida de soportes y documentos que contengan datos de carácter personal, fuera de las instalaciones u oficinas bajo el control del responsable, deberá ser autorizada por éste, o encontrarse debidamente autorizada en el documento de seguridad.

En el traslado de soportes físicos y electrónicos se adoptarán medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

Siempre que vaya a desecharse cualquier soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

g) Copias de respaldo y recuperación:

Deberán establecerse procedimientos para la realización de copias de respaldo y su periodicidad. En caso de que los datos personales se encuentren en soporte físico, se procurará que el respaldo se efectúe mediante la digitalización de los documentos.

Asimismo, para soportes electrónicos se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida involuntaria o destrucción accidental.

El responsable se encargará de verificar, al menos, cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

II. Nivel Medio. El nivel de seguridad medio es aplicable a los sistemas de datos personales relativos a la comisión de infracciones administrativas o penales, hacienda pública, servicios financieros, datos patrimoniales, así como a los sistemas que contengan datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo.

Este nivel, además de las medidas de seguridad previstas para el nivel básico, deberá comprender:

a) Responsable de seguridad:

El responsable designará uno o varios responsables de seguridad para coordinar y controlar las medidas definidas en el documento de seguridad. Esta designación podrá ser única para todos los sistemas de datos en posesión del ente público, o diferenciada, dependiendo de los métodos de organización y tratamiento de los mismos. En todo caso dicha circunstancia deberá especificarse en el documento de seguridad.

En ningún caso esta designación supone una delegación de las facultades y atribuciones que corresponden al responsable del sistema de datos personales de acuerdo con la Ley y los Lineamientos.

b) Auditoría:

Las medidas de seguridad implementadas para la protección de los sistemas de datos personales se someterán a una auditoría interna o externa, mediante la que se verifique el cumplimiento de la Ley, de los presentes Lineamientos y demás procedimientos vigentes en materia de seguridad de datos, al menos, cada dos años.

El informe de resultados de la auditoría deberá dictaminar sobre la adecuación de las medidas de seguridad previstas en los Lineamientos, así como en las recomendaciones, que en su caso, haya emitido el Instituto. Además, deberá identificar sus deficiencias y proponer las medidas preventivas, correctivas o complementarias necesarias.

El informe de auditoría deberá ser comunicado por el responsable al Instituto dentro de los 20 días hábiles siguientes a su emisión. Asimismo, se deberá informar al Instituto de la adopción de las medidas correctivas derivadas de la auditoría en el plazo referido, a partir de que éstas hayan sido atendidas.

c) Control de acceso físico:

El acceso a las instalaciones donde se encuentren los sistemas de datos personales, ya sea en soporte físico o electrónico, deberá permi-

tirse exclusivamente a quienes estén expresamente autorizados en el documento de seguridad.

d) Pruebas con datos reales:

Las pruebas que se lleven a cabo con efecto de verificar la correcta aplicación y funcionamiento de los procedimientos para la obtención de copias de respaldo y de recuperación de los datos, anteriores a la implantación o modificación de los sistemas informáticos que traten sistemas de datos personales, no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de datos tratados. Si se realizan pruebas con datos reales, se elaborará con anterioridad una copia de respaldo.

III. Nivel Alto. El nivel de seguridad alto es aplicable a los sistemas de datos personales que contengan datos relativos a la ideología, religión, creencias, afiliación política, origen racial o étnico, salud, biométricos, genéticos o vida sexual, así como los que contengan datos recabados para fines policiales, de seguridad, prevención, investigación y persecución de delitos.

Este nivel, además de las medidas de seguridad previstas para el nivel básico y medio, deberá comprender:

a) Distribución de soportes:

La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos, o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su traslado o transmisión.

b) Registro de acceso:

El acceso a los sistemas de datos personales se limitará exclusivamente al personal autorizado, estableciendo mecanismos que permitan identificar los accesos realizados en el caso en que los sistemas puedan ser utilizados por múltiples autorizados.

Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad correspondiente, sin que se permita la desactivación o manipulación de los mismos.

De cada acceso se guardarán, al menos, la identificación del usuario, la fecha y hora en que se realizó, el sistema accedido, el tipo de acceso y si éste fue autorizado o denegado.

El periodo de conservación de los datos consignados en el registro de acceso será de, al menos, dos años.

c) Telecomunicaciones:

La transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulable por terceros.

Notificación del nivel de seguridad

17. Los responsables sólo deberán comunicar al Instituto el nivel de seguridad aplicable a los sistemas de datos personales para su registro.

CAPÍTULO III. DEL TRATAMIENTO DE DATOS PERSONALES

Principios

18. En el tratamiento de los datos personales los entes públicos deberán observar los principios de licitud, consentimiento, calidad de los datos, confidencialidad, seguridad, disponibilidad y temporalidad que establece el artículo 5 de la Ley.

19. Para los efectos de la Ley y de los presentes Lineamientos se entenderá que:

I. Con relación al principio de licitud se considerará que la finalidad es distinta o incompatible cuando el tratamiento de los datos personales no coincida con los motivos para los cuales fueron recabados.

II. Con relación al principio de consentimiento se entenderá que éste es:

Libre: Cuando es obtenido sin la intervención de vicio alguno de la voluntad;

Inequívoco: Cuando existe expresamente una acción que implique su otorgamiento;

Específico: Cuando se otorga referido a una determinada finalidad; e

Informado: Cuando se otorga con conocimiento de las finalidades para las que el mismo se produce.

III. Con relación al principio de calidad de los datos, el tratamiento de los datos personales deberá ser:

Cierto: Cuando los datos se mantienen actualizados de tal manera que no se altere la veracidad de la información que traiga como consecuencia que el titular se vea afectado por dicha situación;

Adecuado: Cuando se observa una relación proporcional entre los datos recabados y la finalidad del tratamiento;

Pertinente: Cuando es realizado por el personal autorizado para el cumplimiento de las atribuciones de los entes públicos que los hayan recabado; e

No excesivo: Cuando la información solicitada al titular de los datos es la estrictamente necesaria para cumplir con los fines para los cuales se hubieran recabado.

IV. Con relación al principio de confidencialidad, se entenderá que los datos personales son:

Irrenunciables: El interesado está imposibilitado de privarse voluntariamente de las garantías que le otorga la legislación en materia de protección de datos personales;

Intransferibles: El interesado es el único titular de los datos y éstos no pueden ser cedidos a otra persona; e

Indelegables: Sólo el interesado tiene la facultad de decidir a quién transmite sus datos personales.

El deber de secrecía y el de confidencialidad se considerarán equiparables.

Deber de confidencialidad

20. El responsable y toda persona que intervenga en cualquier fase del tratamiento de los datos personales en posesión de los entes públicos están obligados a guardar absoluta confidencialidad respecto de los mismos, obligación que subsistirá aun después de finalizada la relación por la cual se dio el tratamiento.

Finalidad determinada

21. Los datos personales en posesión de los entes públicos deberán tratarse únicamente para la finalidad para la cual fueron obtenidos. Dicha finalidad deber ser explícita, determinada y legal.

Deber de actualización

22. Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario para responder con veracidad a la situación actual de su titular. Cuando los datos de carácter personal sometidos a tratamiento sean inexactos o incompletos, el responsable procederá de oficio a actualizarlos en el momento en que tenga conocimiento de la inexactitud, siempre que cuente con la documentación que justifique la actualización de dichos datos. En el caso de que los datos hubieren sido cedidos previamente, el responsable deberá comunicarlo a los cesionarios dentro del plazo de diez días hábiles.

Consentimiento

23. El responsable deberá obtener el consentimiento del interesado para el tratamiento de sus datos personales, salvo en aquellos supuestos en que el mismo no sea exigible con arreglo a lo dispuesto en el artículo 16 de la Ley.

El consentimiento del interesado deberá ir referido a un tratamiento específico, con delimitaciones de temporalidad y finalidad.

Destino de los datos

24. Cuando se solicite el consentimiento del interesado para la cesión de sus datos, éste deberá ser informado de forma que conozca

inequívocamente la finalidad a la que se destinarán los datos respecto de cuya comunicación se solicita el consentimiento, así como el tipo de actividad desarrollada por el cesionario. En caso contrario, el consentimiento será nulo.

Menores o incapaces

25. En caso de que el ente público requiera obtener datos personales de menores de edad o incapaces, el responsable, o en su defecto, el encargado, deberá cerciorarse de que quien otorga el consentimiento es la persona que ejerce la patria potestad, tutela o la representación legal del menor o incapaz de que se trate en términos del Código Civil para el Distrito Federal.

Forma de recabar el consentimiento

26. El responsable deberá dirigirse al interesado por escrito para hacer de su conocimiento los aspectos a que se refiere el artículo 9 de la Ley, concediéndole un plazo de quince días hábiles para manifestar su negativa al tratamiento, bajo la advertencia de que en caso de no pronunciarse a tal efecto se entenderá que consiente el tratamiento de sus datos personales. Para efectos de cumplir con el deber de información, el responsable deberá incorporar al escrito la Leyenda a que hace referencia el numeral 13 de estos Lineamientos.

En caso de los sistemas de datos creados con anterioridad a la entrada en vigor de la Ley, así como en los casos y excepciones señalados en el artículo 16 de la misma, no se requerirá la notificación a la que se hace referencia en el párrafo anterior, salvo que los datos reciban un tratamiento distinto a aquel para el que fueron recabados.

La comunicación podrá realizarse en el domicilio del ente público; por correo electrónico o por correo certificado.

Revocación del consentimiento

27. El interesado podrá revocar su consentimiento de conformidad con lo dispuesto en el artículo 16 de la Ley, mediante solicitud presentada ante la Oficina de Información Pública que corresponda, a través de los

formatos que para tal efecto emita el Instituto. La solicitud deberá ser acompañada de un medio de identificación oficial.

Además de cumplir con los requisitos establecidos en el artículo 34 de la Ley, los interesados deberán, en su caso, especificar la finalidad para la cual se revoca el consentimiento para tratar sus datos personales.

La Oficina de Información Pública realizará las gestiones necesarias ante el responsable que corresponda hasta la culminación del procedimiento que se hará de conformidad con lo dispuesto en el artículo 32 de la Ley.

Efectos de la revocación

28. En caso de que el responsable determine que la solicitud de revocación del consentimiento es procedente, éste deberá cesar en el tratamiento de los datos, sin perjuicio de la obligación de bloquear los datos conforme a la Ley y estos Lineamientos.

En el caso de que los datos hubieren sido cedidos previamente, el responsable, una vez revocado el consentimiento, deberá comunicarlo a los cesionarios dentro del plazo de diez días hábiles para que procedan de conformidad con el primer párrafo de este numeral.

Ante la improcedencia de la revocación del consentimiento, el interesado podrá ejercer su derecho de cancelación, conforme a la Ley y los Lineamientos.

Tratamiento ilícito de datos personales

29. El Instituto podrá, en los supuestos a que hace referencia el artículo 17 de la Ley, requerir, mediante resolución fundada y motivada del Pleno, que los responsables de sistemas de datos personales suspendan la utilización o cesión de determinados datos.

El requerimiento deberá ser atendido dentro del plazo improrrogable de cinco días hábiles al término del cual el responsable deberá rendir un informe en el cual señale las medidas adoptadas para la suspensión y en el que alegue lo que a su derecho convenga.

Transcurrido el plazo, el Instituto deberá emitir una resolución, dentro del término de quince días hábiles, en la que podrá:

Emitir recomendaciones en las que requiera al ente público se subsanen las irregularidades detectadas, mismas que tendrán que ser solventadas dentro del plazo y condiciones que al efecto se establezcan;

Requerir al responsable la cancelación o rectificación de determinados datos contenidos en el sistema que corresponda;

Requerir que el responsable modifique el sistema a efecto de que se ajuste a lo establecido en la Ley y demás normativa aplicable; y

Determinar que no hay elementos que permitan establecer que se actualizan los supuestos a que hace referencia el artículo 17 de la Ley.

En los supuestos previstos en las fracciones I a la IV, del presente numeral, el Instituto podrá ordenar el levantamiento de la suspensión y el archivo del expediente.

30. En caso de que el requerimiento de suspensión fuera desatendido, el Instituto, mediante resolución fundada y motivada del Pleno, podrá requerir la inmovilización del sistema correspondiente, con el único fin de restaurar los derechos de las personas afectadas, lo que se hará de conformidad con el lineamiento anterior.

Si el requerimiento de inmovilización del sistema fuera desatendido, el Instituto dará vista a la autoridad competente para el deslinde de responsabilidades.

El Instituto podrá evaluar el cumplimiento de la actuación del ente público mediante la realización de visitas de inspección en los términos de la Ley y estos Lineamientos.

Cuando el Instituto advierta una presunta infracción a la Ley dará vista al órgano interno de control o su equivalente para que determine lo que en derecho corresponda.

Cancelación de datos personales por los entes públicos

31. Los datos de carácter personal serán cancelados, de oficio o a petición del interesado, una vez que hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hayan sido recabados. Sin embargo, deberán conservarse durante el tiempo en que pueda exigir-

se algún tipo de responsabilidad derivada de una relación u obligación jurídica, o de la ejecución de un contrato.

Una vez cumplido el plazo a que se refiere el párrafo anterior, los datos sólo podrán conservarse previa disociación de los mismos, sin perjuicio de la obligación de bloqueo prevista en la Ley y estos Lineamientos.

Plazos para la cancelación

32. Los datos personales que hayan sido objeto de tratamiento y no contengan valores históricos, científicos o estadísticos, deberán ser cancelados del sistema de datos personales, teniendo en cuenta los siguientes plazos:

El que se haya establecido en el formato físico o electrónico por medio del cual se recabaron;

El establecido por las disposiciones aplicables; y

El establecido en el instrumento jurídico formalizado entre un tercero y el ente público.

Cesión de datos personales

33. La cesión de datos personales sólo podrá realizarse cuando el cesionario garantice por escrito un nivel de protección similar al empleado en el sistema de datos personales, y que se haya consignado en el documento de seguridad. El cesionario de los datos personales quedará sujeto a las mismas obligaciones que corresponden al responsable que los transfirió.

Seguridad en la cesión

34. El carácter adecuado de las medidas de seguridad que ofrece el cesionario se evaluará atendiendo las circunstancias que concurran en la transferencia, y en específico se tomará en consideración la naturaleza de los datos personales, la finalidad y la duración del tratamiento.

CAPÍTULO IV. DE LAS OBLIGACIONES DE LOS ENTES PÚBLICOS

35. Los responsables y encargados están obligados a cumplir con lo dispuesto en la Ley, los Lineamientos y el documento de seguridad aplicable para cada sistema de datos personales.

El titular del ente público tiene la obligación de designar al o los servidores públicos responsables de los sistemas de datos personales, quienes deberán estar adscritos a la unidad administrativa en la que se concrete la competencia material del sistema. Los responsables tienen la atribución de decidir sobre el contenido y finalidad de los sistemas de datos personales.

El titular del ente público también deberá designar al servidor público que fungirá como enlace entre el ente y el Instituto.

El servidor público designado como enlace también coordinará a los responsables de los sistemas de datos personales al interior del ente público.

Los responsables, encargados y usuarios deberán estar obligados a cumplir con lo dispuesto en la Ley, los Lineamientos y el documento de seguridad aplicable para cada sistema de datos personales.

Tratamiento por usuarios

36. En caso de que el tratamiento de datos personales sea por cuenta de usuarios, el responsable deberá asegurarse que dicha acción esté regulada en un contrato, que deberá constar por escrito, o en alguna otra forma que permita acreditar su celebración y contenido, en el cual se establecerá que el usuario únicamente tratará los datos conforme a las instrucciones del responsable, que no los aplicará o utilizará con una finalidad distinta a la que figura en el contrato, ni los comunicará a otras personas.

En el contrato se estipularán las medidas de seguridad que se deban implementar para el tratamiento por el usuario.

Concluida la relación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable.

Informe anual

37. El informe a que hace referencia la fracción III del artículo 21 de la Ley deberá contener los siguientes apartados:

Número de solicitudes de acceso, rectificación, cancelación y oposición de datos personales presentadas ante el ente público, así como su resultado;

El tiempo de respuesta a la solicitud;

El estado que guardan las denuncias presentadas ante los órganos internos de control, así como de las vistas dadas por el Instituto;

Dificultades observadas en el cumplimiento de la Ley;

Descripción de los recursos públicos utilizados en la materia;

Sistemas de datos personales creados, modificados y/o suprimidos;

Acciones desarrolladas para dar cumplimiento a las disposiciones contenidas en la Ley; y

Cesiones de datos personales efectuadas que deberá detallar:

Identificación del sistema mediante número de folio otorgado por el Instituto, del ente cedente y del cesionario;

Finalidad de la cesión;

La mención de si se trata de una cesión total o parcial de un sistema de datos personales y, en su caso, las categorías de datos de que se trate;

Fecha de inicio y término de la cesión y, en su caso, la periodicidad de la misma;

Medio empleado para realizar la cesión;

Medidas y niveles de seguridad empleados para la cesión;

Obligaciones al término del tratamiento; y

El nivel de seguridad aplicado por el cesionario.

Enlace

38. El servidor público designado como enlace tendrá las siguientes obligaciones:

Coordinar a los responsables de sistemas de datos personales al interior del ente público para el cumplimiento de la Ley, los Lineamientos y demás normativa aplicable;

Supervisar que los responsables mantengan actualizada la inscripción de los sistemas bajo su responsabilidad en el Registro electrónico creado por el Instituto;

Coordinar las acciones en materia de capacitación; y

Remitir el informe a que hace referencia la fracción III del artículo 21 de la Ley.

Encargado

39. El encargado deberá ser una persona que labore en el ente público, en tanto que el usuario es aquella persona física o moral externa al ente público que le presta servicios para tratar datos personales o que implica el tratamiento de los mismos.

El acceso a los sistemas de datos personales por parte de la persona encargada del tratamiento, no se considerará una cesión o delegación de responsabilidades por parte del responsable del sistema.

TÍTULO TERCERO. DE LA AUTORIDAD RESPONSABLE DEL CONTROL Y VIGILANCIA

CAPÍTULO ÚNICO. INSTITUTO DE ACCESO A LA INFORMACIÓN PÚBLICA DEL DISTRITO FEDERAL

Facultad de inspección

40. El Instituto dispondrá de los medios de investigación y de la facultad de intervenir frente a la creación, modificación y supresión de sistemas de datos personales sujetos al ámbito de aplicación de la Ley, que no se ajusten a las disposiciones de la misma, de los presentes Lineamientos y de las demás disposiciones que resulten aplicables.

A tal efecto, tendrá acceso a los sistemas de datos personales, podrá inspeccionarlos y recabar toda la información necesaria para el cumplimiento de su función de control, podrá solicitar la exhibición o el envío

de documentos y datos, así como examinarlos en el lugar en donde se encuentren instalados.

Procedimiento

41. El Instituto, en términos del artículo 24, fracción XVI de la Ley, podrá realizar visitas de inspección, las cuales no podrán referirse a información de acceso restringido, a efecto de evaluar la actuación de los entes públicos, de conformidad con lo siguiente:

Toda visita de inspección deberá ajustarse a los procedimientos y formalidades establecidos en estos Lineamientos;

Los inspectores, al practicar una visita, deberán llevar siempre consigo el Acuerdo del Pleno del Instituto que determinó la diligencia en el que deberá precisarse el ente público que ha de inspeccionarse, el objeto de la visita, el alcance que deba tener y las disposiciones legales que la fundamenten;

Los responsables o encargados del sistema de datos personales objeto de inspección estarán obligados a permitir el acceso y dar facilidades e informes a los inspectores para el desarrollo de su labor;

Al iniciar la visita, el inspector deberá exhibir credencial vigente con fotografía, expedida por el Instituto, que lo acredite para desempeñar dicha función, así como el acuerdo a que se refiere la fracción II de este numeral, de la que deberá dejar copia al responsable del sistema de datos personales de que se trate o a la persona con quien se entienda la diligencia;

De toda visita de inspección se levantará acta circunstanciada, en presencia de dos testigos propuestos por el responsable o servidor público con quien se entienda la diligencia o, en su caso, por quien la practique si aquél se hubiere negado a proponerlos;

De toda acta se dejará copia al servidor público con quien se entendió la diligencia, aunque se hubiere negado a firmar, lo que no afectará la validez de la diligencia ni del documento de que se trate, siempre y cuando el inspector haga constar tal circunstancia en el acta;

En las actas se hará constar:

Identificación del ente público visitado;

Hora, día, mes y año en que se inicie y concluya la diligencia;

Calle, número, población o colonia, teléfono u otra forma de comunicación disponible, delegación y código postal en que se encuentre ubicado el lugar en que se practique la visita;

Número y fecha del acuerdo del Pleno que la motivó;

Nombre y cargo de la persona con quien se entendió la diligencia;

Nombre y cargo de las personas que fungieron como testigos;

Datos relativos a la actuación;

Declaración del visitado, si quiere hacerla; y

Nombre y firma de quienes intervinieron en la diligencia incluyendo los de quien o quienes la hubieren llevado a cabo. Si se negare a firmar el visitado, ello no afectará la validez del acta, debiendo el inspector asentar la razón relativa.

La visita debe entenderse con el responsable del sistema. En caso de que no se encontrara presente, la diligencia se entenderá con el encargado y, en su defecto, con quien se encuentre presente, circunstancia que se hará constar en el acta;

Los visitados a quienes se haya levantado acta de inspección podrán formular observaciones en el acto de la diligencia y ofrecer pruebas en relación a los hechos contenidos en ella, o bien por escrito, así como hacer uso de tal derecho dentro del término de cinco días hábiles siguientes a la fecha en que se hubiere levantado; y

Transcurrido el plazo señalado en el numeral anterior, el Instituto deberá emitir una resolución dentro del término de quince días hábiles en la que podrá:

Determinar que el sistema de datos personales se ajusta a lo establecido en la Ley;

Determinar que existen irregularidades que contravienen lo establecido en la Ley y demás normatividad aplicable, caso en el que formulará recomendaciones al ente público, a efecto de que subsane las inconsistencias detectadas dentro del plazo y condiciones que al efecto se determinen;

El ente público deberá informar por escrito al Instituto, dentro de los cinco días hábiles siguientes a que termine el plazo a que se refiere el

numeral anterior, sobre la atención a las recomendaciones formuladas por el Instituto; y

En caso de que el ente público fuese omiso en presentar los informes o en solventar las recomendaciones, el Instituto, dará vista al órgano interno de control para los efectos legales correspondientes, sin que esta situación lo exima del cumplimiento de las mismas.

En caso de que, en la visita de inspección se advirtiera un posible tratamiento ilícito de los datos personales, se estará a lo dispuesto en los numerales 29 y 30 de los presentes Lineamientos.

TÍTULO CUARTO. DE LOS DERECHOS Y DEL PROCEDIMIENTO PARA SU EJERCICIO

CAPÍTULO ÚNICO. DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN

42. Los derechos de acceso, rectificación, cancelación y oposición son personalísimos y, serán ejercidos directamente por el interesado o su representante legal.

Procedimientos

43. Los entes públicos deberán observar, de forma complementaria a lo establecido en la Ley y en los Lineamientos para la gestión de solicitudes de información pública y de datos personales a través del sistema INFOMEX del Distrito Federal, las disposiciones previstas en este título.

En caso de que la solicitud presentada no corresponda a una solicitud de acceso, rectificación, cancelación u oposición sobre datos de carácter personal la Oficina de Información Pública deberá notificarlo dentro del plazo de cinco días hábiles al solicitante y, en su caso, orientarlo para que presente una solicitud de información pública o realice el trámite que corresponda.

Derecho de acceso

44. El derecho de acceso es la prerrogativa del interesado a obtener información acerca de si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso, se esté realizando, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos.

45. El interesado podrá, a través del derecho de acceso, obtener información relativa a datos concretos, a datos incluidos en un determinado sistema o la totalidad de los datos sometidos a tratamiento en los sistemas de datos personales en posesión de un ente público.

Derecho de rectificación

46. El derecho de rectificación es la prerrogativa del interesado a que se modifiquen los datos que resulten inexactos o incompletos, con respecto a la finalidad para la cual fueron obtenidos. Los datos serán considerados exactos si corresponden a la situación actual del interesado.

47. La solicitud de rectificación deberá indicar qué datos se requiere sean rectificados o completados y se acompañará de la documentación que justifique lo solicitado.

Derecho de cancelación

48. El derecho de cancelación es la prerrogativa del interesado a solicitar que se eliminen los datos que resulten inadecuados o excesivos en el sistema de datos personales de que se trate, sin perjuicio de la obligación de bloquear los datos conforme a la Ley y a los presentes Lineamientos.

Para efectos del párrafo anterior, se considerará que los datos son inadecuados, cuando estos no guarden una relación con el ámbito de aplicación y finalidad por la cual fueron recabados, o bien, si dejaron de ser necesarios con respecto a dicha finalidad; así mismo se considerarán como excesivos, si los datos obtenidos son más de los estrictamente necesarios en relación a dicha finalidad.

El interesado también podrá solicitar la cancelación de sus datos cuando el tratamiento de los mismos no se ajuste a lo dispuesto en la Ley o en estos Lineamientos.

49. En la solicitud de cancelación, el interesado deberá indicar a qué datos se refiere, aportando, en su caso, la documentación que justifique las razones por las cuales considera que el tratamiento no se ajusta a lo dispuesto en la Ley.

50. Los derechos de rectificación y cancelación no procederán en los supuestos en que así lo disponga una Ley.

Derecho de oposición

51. El derecho de oposición es la prerrogativa del interesado a solicitar que no se lleve a cabo el tratamiento de sus datos personales para un fin determinado o se cese en el mismo, cuando no sea necesario otorgar el consentimiento para el tratamiento en términos de lo dispuesto por el artículo 16 de la Ley, como consecuencia de un motivo legítimo y fundado del interesado y siempre que una Ley no disponga lo contrario.

52. En caso de que la oposición sea procedente, dará lugar a la cancelación del dato, previo bloqueo, mientras transcurren los plazos previstos, a efecto de depurar las responsabilidades que correspondan.

TRANSITORIOS

PRIMERO. Los presentes Lineamientos entrarán en vigor al día siguiente de su publicación en la Gaceta Oficial del Distrito Federal.

SEGUNDO. El titular del ente público deberá designar al enlace y notificarlo al Instituto para su registro dentro de los quince días hábiles posteriores a la entrada en vigor de los presentes Lineamientos.

TERCERO. Los responsables deberán inscribir los sistemas de datos personales bajo su custodia dentro de los noventa días hábiles siguientes a la entrada en vigor de estos Lineamientos en el Registro Electrónico de Sistemas de Datos Personales.

Bibliografía

Alberch, Ramón, y otros. *Archivos y cultura: manual de dinamización*, Ramón Alberch [et al.], Gijón: Trea [2001]; 173 p.; 22 cm.

Abad Amorós, Ma. Rosa. "La protección de datos" en: *Derecho de la Información*, BEL Y CORREIDORA (coords.), Ariel, 2003, España.

López-Ayllón, Sergio. "La reforma y sus efectos legislativos", en: SALAZAR UGARTE, Pedro (coord.), *El derecho de acceso a la información en la constitución mexicana: razones significados y consecuencias*, UNAM, IFAI, México.

Lucas Murillo de la Cueva, Pablo. "La protección de datos en la administración de justicia", en: *Derecho a la intimidad y nuevas tecnologías*, *Cuadernos de Derecho Judicial*, Consejo General del Poder Judicial, Madrid, España, 2004.

Lucas Murillo de la Cueva, Pablo. *El derecho a la autodeterminación informativa*, Tecnos, Madrid, España, 1990.

Troncoso Reigada, Antonio. "La declaración de los ficheros de datos personales: acerca de un modelo centralizado o descentralizado" (en línea). Madrid: "Opinión de los expertos" *Revista digital: Datospersonales.org*, Madrid, APDCM, marzo 2009. Número 38.

Villanueva, Ernesto. *Derecho de acceso a la información pública en Latinoamérica*, UNAM, México, 2003.

Glosario

Autentificación: Comprobación de la identidad de aquella persona autorizada para el tratamiento de datos personales.

Bloqueo: Identificación y conservación de datos personales con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo, legal o contractual, de prescripción de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación del sistema a que correspondan.

Cancelación: Eliminación de determinados datos de un sistema de datos personales previo bloqueo de los mismos.

Cesionario: Persona física o moral, pública o privada, a la que un ente público realice una cesión de datos personales.

Cesión de datos personales: Toda obtención de datos resultante de la consulta de un archivo, registro, base o banco de datos, una publicación de los datos contenidos en él, su interconexión con otros ficheros y la comunicación de datos realizada por una persona distinta a la interesada, así como la transferencia o comunicación de datos realizada entre entes públicos.

Cifrado de datos: El cifrado se puede entender como el hecho de guardar algo valioso dentro de una caja fuerte cerrada con llave. Los datos confidenciales se cifran con un algoritmo de cifrado y una clave que los hace ilegibles si no se conoce dicha clave. Las claves de cifrado de datos se determinan en el momento de realizar la conexión entre los equipos. El uso del cifrado de datos puede iniciarse en su equipo o en el servidor al que se conecta.

Consentimiento: Autorización o permiso para que se haga algo.

Copia de respaldo: Copia de los datos de un archivo informático en un soporte que posibilite su recuperación.

Datos disociados: Aquellos que no permiten la identificación de un afectado o interesado.

Datos personales: La información numérica, alfabética, gráfica, acústica o de cualquier otro tipo concerniente a una persona física, identificada o identificable. Tal y como son, de manera enunciativa y no limitativa: el origen étnico o racial, características físicas, morales o emocionales, la vida afectiva y familiar, el domicilio y teléfono particular, correo electrónico no oficial, patrimonio, ideología y opiniones políticas, creencias, convicciones religiosas y filosóficas, estado de salud,

preferencia sexual, la huella digital, el ADN y el número de seguridad social, y análogos.

Documentos: Los expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas, o bien cualquier otro registro en posesión de los entes públicos sin importar su fuente o fecha de elaboración. Los documentos podrán estar en cualquier soporte, demás análogos escrito, impreso, sonoro, visual, electrónico, informático u holográfico.

Documento de seguridad: Instrumento que establece las medidas y procedimientos administrativos, físicos y técnicos de seguridad aplicables a los sistemas de datos personales necesarios para garantizar la protección, confidencialidad, integridad y disponibilidad de los datos contenidos en dichos sistemas.

Encargado: Servidor público que en ejercicio de sus atribuciones, realiza tratamiento de datos personales de forma cotidiana.

Enlace: Servidor público que funge como vínculo entre el ente público y el Instituto para atender los asuntos relativos a la Ley de Protección de Datos Personales para el D. F.

Ente Público: La Asamblea Legislativa del Distrito Federal; el Tribunal Superior de Justicia del Distrito Federal; El Tribunal de lo Contencioso Administrativo del Distrito Federal; El Tribunal Electoral del Distrito Federal; el Instituto Electoral del Distrito Federal; la Comisión de Derechos Humanos del Distrito Federal; la Junta de Conciliación y Arbitraje del Distrito Federal; la Jefatura de Gobierno del Distrito Federal; las Dependencias, Órganos Desconcentrados, Órganos Político Administrativos y Entidades de la Administración Pública del Distrito Federal; los Órganos Autónomos por Ley; los partidos políticos, asociaciones y agrupaciones políticas; así como aquellos que la legislación local reconozca como de interés público y ejerzan gasto público; y los entes equivalentes a personas jurídicas de derecho público o privado, ya sea que en ejercicio de sus actividades actúen en auxilio de los órganos antes citados o ejerzan gasto público.

Fuente de acceso público: Aquella cuya consulta pueda ser realizada por cualquier persona, no impedida por una norma limitativa, sin más exigencia que, en su caso, el pago que genere el acceso a determinado medio de información. Tendrán el carácter de fuentes de acceso público los Registros Públicos, los diarios, gacetas y boletines gubernamentales, así como otros medios oficiales de difusión.

Incidencia: Cualquier anomalía que afecte o pudiera afectar la seguridad de los datos personales.

Inequívoco: Que no admite duda o equivocación.

INFOMEX: Sistema electrónico mediante el cual las personas podrán presentar sus solicitudes de acceso a la información pública y de acceso, rectificación, cancelación y oposición de datos personales y es el sistema único para el registro y captura de todas las solicitudes recibidas por los entes públicos a través de los medios señalados en la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal y la Ley de Protección de Datos Personales para el Distrito Federal, así como para la recepción de los recursos de revisión interpuestos a través del propio sistema.

Interesado: Persona física titular de los datos personales que sean objeto del tratamiento al que se refiere la presente Ley.

Inmovilización: Medida cautelar que consiste en la interrupción temporal en el uso de un sistema de datos personales ordenada por el Instituto en los supuestos de tratamiento ilícito de datos de carácter personal.

Oficina de Información Pública: La unidad administrativa receptora de las solicitudes de acceso, rectificación, cancelación y oposición de datos personales en posesión de los entes públicos, a cuya tutela estará el trámite de las mismas, conforme a lo establecido en esta Ley y en los lineamientos que al efecto expida el Instituto.

Procedimiento de disociación: Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a una persona física identificada o identificable.

Registro Electrónico de Sistemas de Datos Personales: Aplicación informática desarrollada por el Instituto para la inscripción de los sistemas de datos personales en posesión de los entes públicos.

Responsable: El servidor público de la unidad administrativa a la que se encuentre adscrito el sistema de datos personales, designado por el titular del ente público, que decide sobre el tratamiento de datos personales, así como el contenido y finalidad de los sistemas de datos personales.

Responsable de seguridad: Persona a la que el responsable del sistema de datos personales asigna formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

Revocar: Dejar sin efecto una concesión, mandato o resolución.

Sistema de Datos Personales: Conjunto organizado de datos personales que estén en posesión de los entes públicos, contenidos en archivos, registros, ficheros, bases o bancos de datos, que permita el acceso a datos con arreglo a criterios determinados, cualquiera que fuere la modalidad de su creación, almacenamiento, organización o acceso.

Soporte electrónico: Son los medios de almacenamiento inteligibles sólo mediante el uso de algún aparato con circuitos electrónicos que procese su contenido para examinar, modificar o almacenar los datos; es decir, cintas magnéticas de audio, vídeo y datos, fichas de microfilm, discos ópticos (CDs y DVDs), discos magneto-ópticos, discos magnéticos (flexibles y duros) y demás medios de almacenamiento masivo no volátil.

Soporte físico: Son los medios de almacenamiento inteligibles a simple vista, es decir, que no requieren de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos; es decir, documentos, oficios, formularios impresos llenados “a mano” o “a máquina”, fotografías, placas radiológicas, carpetas, expedientes, demás análogos.

Supresión: Eliminación de un sistema de datos personales mediante acuerdo publicado en la Gaceta Oficial del Distrito Federal.

Suspensión: Medida cautelar ordenada por el Instituto de Acceso a la Información Pública del D.F. que consiste en la interrupción temporal en el tratamiento de determinados datos personales contenidos en un sistema de datos personales.

Transmisión de datos: Cualquier traslado, comunicación, envío, entrega o divulgación de los datos.

Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos automatizados o físicos, aplicados a los sistemas de datos personales, relacionados con la obtención, registro, organización, conservación, elaboración, utilización, cesión, difusión, interconexión o cualquier otra forma que permita obtener información de los mismos y facilite al interesado el acceso, rectificación, cancelación u oposición de sus datos.

Usuario: Aquel autorizado por el ente público para prestarle servicios para el tratamiento de datos personales.

Vulneración: Transgresión, quebranto, violación de una ley o precepto.

Bibliografía del Glosario

Ley de Protección de Datos Personales para el Distrito Federal 2009.

Lineamientos de Protección de Datos Personales para el Distrito Federal 2009.

Del Peso Navarro, Emilio; Ramos González, Miguel Ángel; Del Peso Ruiz, Margarita; Del Peso Ruiz, Mar. 2008, *Nuevo Reglamento de Protección de Datos de Carácter Personal, Medidas de Seguridad*, Ediciones Díaz de Santos.

http://technet.microsoft.com/es-es/library/cc785633(WS.10).aspx

http://www.wordreference.com/definicion/consentimiento

Notas

1. http://www.webjuridico.net/hoi/hoi06.htm

2. Rysdall, R. “Protección de datos y el Convenio Europeo de los Derechos Humanos”, Discurso de apertura de la XIII Conferencia de Comisarios de Protección de Datos, Novática, marzo de 1992, p.9.

3. Otero Parga, Milagros. Consideraciones en torno al derecho a la intimidad, en Los derechos fundamentales y libertades públicas (XII Jornadas de Estudio de la Dirección General del Servicio Jurídico del Estado), Ministerio de Justicia, Madrid, 1992, vol. I, pp. 697-698.

4. Artículo 2.a de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995.

5. En el análisis de estos componentes seguimos, en lo fundamental, el Dictamen 4/2007 sobre el concepto de datos personales adoptado el 20 de junio por el GRUPO DE TRABAJO DEL ARTÍCULO 29, creado en virtud del artículo 29 de la Directiva 95/46/CE. Se trata de un organismo de la UE, de carácter consultivo e independiente, para la protección de datos y el derecho a la intimidad. Se sugiere su consulta para profundizar en el tema. El documento está disponible en: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_es.pdf

6. El artículo 10 de la LPDPDF considera como datos sensibles a: el origen étnico o racial, características morales o emocionales, ideología y opiniones políticas, creencias religiosas, filosóficas y preferencia sexual.

7. Documento nº WP 105 del Grupo de trabajo: “Documento de trabajo sobre las cuestiones relativas a la protección de datos relacionadas con la tecnología RFID”, adoptado el 19.1.2005, p. 8.

8. Artículo 22.

9. Publicada en el Periódico Oficial “El Estado de Colima” el 21 de junio de 2003.

10. Por ejemplo, la Ley argentina aplica tanto a personas físicas como a personas morales y define a los datos personales como información de cualquier tipo referida a personas físicas o de existencia ideal (jurídicas) determinadas (identificadas) o determinables (identificables).

11. Lucas Murillo de la Cueva, “La protección de datos en la administración de justicia”, en: Derecho a la intimidad y nuevas tecnologías, Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, Madrid, España, 2004, p.233.

12. **Abad Amorós,** Ma. Rosa. “La protección de datos” en: Derecho de la Información, BEL Y CORREIDORA (Coords.), Ariel, 2003, España, p.357.

13. **Villanueva,** Ernesto. *Derecho de acceso a la información pública en Latinoamérica*, UNAM, México, 2003, p. XXV.

14. **Arbeláez de Tobón,** Lucía. “Transparencia, derechos fundamentales y la Internet en el Poder Judicial de Colombia”, Ponencia presentada en el Seminario-Taller sobre la INTERNET Y SISTEMA JUDICIAL EN AMERICA LATINA Y EL CARIBE.

15. Expresión latina que significa “a la ciudad y al mundo entero”. Se emplea para expresar que cierta cosa se hace llegar a todas partes y que específicamente se publica a los cuatro vientos.

16. **Ornelas Núñez,** Lina y López Ayllón, Sergio. Documento “La recepción del derecho a la protección de datos en México: Breve descripción de su origen y estatus legislativo”.

17. **Velasco San Martín,** Cristos. “Privacidad y protección de datos personales en *Internet ¿Es necesario contar con una regulación específica en México?*, *Boletín de Política Informática*, No. 1, 2003, pp.4-5.

18. Organización para la Cooperación y Desarrollo Económico, organización de cooperación internacional, compuesta por 30 Estados, cuyo objetivo es coordinar sus políticas económicas y sociales.

19. **Bayo Delgado,** Joaquín. “Derecho comunitario sobre protección de datos” en GÓMEZ MARTÍNEZ, (dir.) *Derecho a la intimidad y nuevas tecnologías*, *Cuadernos de Derecho Judicial* IX-2004, Consejo General del Poder Judicial, 2004, p.50.

20. Abrogar es abolir o dejar sin efecto una norma vigente. Cuando se abroga una norma ésta se elimina completamente. www.lenguajeciudadano.gob.mx (13 de octubre de 2008).

21. Sobre este particular, los asambleístas consideraron que por su relevancia estas materias deberían contar con una ley específica. La LPDPDF se publicó en la *Gaceta Oficial del Distrito Federal* el 3 de octubre de 2008 y la Ley de Archivos local el 8 del mismo mes y año.

22. La LPDPDF también recoge el principio denominado “derecho de información” o “deber de información”, si bien no se refiere a él dentro del artículo 5 si lo contempla en el artículo 9.

23. **López-Ayllón,** Sergio. “La reforma y sus efectos legislativos”, en: SALAZAR UGARTE, Pedro (Coord.), *El derecho de acceso a la información en la Constitución mexicana: razones significados y consecuencias*, UNAM, IFAI, México, 2008, p.18.

24. El procedimiento de disociación consiste en todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a una persona física identificada o identificable.

25. Capítulo II del Título Segundo “De la tutela de datos personales”.

26. **Troncoso Reigada,** Antonio. “La declaración de los ficheros de datos personales: acerca de un modelo centralizado o descentralizado”, (en línea). Madrid: “Opinión de los expertos” *Revista digital: Datospersonales.org*, Madrid, APDCM, marzo 2009. Número 38.

http://www.madrid.org/cs/Satellite?c=CM_Revista_FP&cid=1142540478587&esArticulo=true&idRevistaElegida=1142527411030&language=es&pagename=RevistaDatosPersonales%2FPage%2Fhome_RDP&siteName=RevistaDatosPersonales (consulta: 20 julio 2009).

27. Artículo 7 LPDPDF.

28. Las medidas de seguridad se regulan en el Capítulo III, del Título Segundo "De la tutela de datos personales" de la LPDPDF (artículos 13 al 15).

29. En México los criterios científicos, tecnológicos y administrativos obligatorios en la elaboración, integración, uso y archivo del expediente clínico están contenidos en la Norma Oficial Mexicana: NOM-168-SSA1-1998 DEL EXPEDIENTE CLÍNICO.

30. El Instituto Federal de Acceso a la Información Pública (IFAI) cuenta con un "Estudio sobre expedientes clínicos" disponible en: http://www.ifai.org.mx/SitiosInteres/ligas-Sitios

31. Como es el caso de la Agencia Española de Protección de Datos que tiene facultades para imponer multas millonarias. www.agpd.es

32. Sobre este último punto existe un procedimiento específico en los Lineamientos (numeral 41).

33. La propia LPDPDF hace referencia a la Ley Federal de Responsabilidades de los Servidores Públicos, la cual en su artículo 78 establece el plazo de prescripción para imponer sanciones.

34. Sobre el recurso de revisión consultar: http://www.infodf.org.mx/capacitacion/publicacionesDCCT/Recursoderevision/recursoderevision.pdf

35. El plazo será de 20 días si el ente no presenta el informe de ley o de 10 días si el recurso se presenta por falta de respuesta.

Evalúate en Línea

Te recordamos que si ya concluiste el curso a través de este Manual de Autoformación y deseas obtener una **Constancia de Acreditación validada por el InfoDF**, debes presentar tus evaluaciones a través del Aula Virtual de Aprendizaje (AVA), localizada en la página de internet www.aula-infodf.org/aulavirtual/.

Una vez que hayas concluido las evaluaciones correspondientes a este curso, con las calificaciones requeridas (10 en cada tema), el InfoDF te otorgará una Constancia de Acreditación.

Para cualquier duda a este respecto, puedes comunicarte al teléfono **56 36 21 20 Ext**. **159**.

Colección Capacitación a Distancia
05

Instituto de Acceso a la Información Pública del Distrito Federal.
Manual de Autoformación sobre la Ley de Protección de Datos Personales para el Distrito Federal.
Diciembre de 2009.
Corporación Mexicana de Impresión S. A. de C. V.
General Victoriano Zepeda No. 22 Col. Observatorio,
C. P. 11860, México, D. F.
El tiraje fue de 2,000 ejemplares impresos en papel bond de 90 g
y forros en couché de 250 g.
Fuentes tipográficas: Arial, Arial Black, Carta, Gill Sans MT,
Imprint MT Shadow y Zapf Ding bats.
Cuidado de la edición: Dirección de Capacitación
y Cultura de la Transparencia.