**Derecho a la Protección de Datos Personales.**

**Tema 1. Derecho a la Intimidad**

Entendamos 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.

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.**

**MÁS QUE LA PROTECCIÓN DE DATOS ES: 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.**

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

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 p**rincipio de autodeterminación informativa o de poder de control sobre los datos personales.**

Se puede definir como **aquel derecho de la personalidad**, 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.**

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

|  |  |
| --- | --- |
|

|  |
| --- |
| **Tema 2. Derecho a la Privacidad** |

 |

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

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.

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?**

 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.

**Dato Personal**: 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**.

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.

|  |
| --- |
| ***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.*****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:

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

**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. (**No es necesario que determinada información sea verídica o probada para que se considere dato personal.)

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.

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.

En cuanto al componente **“sobre”** se considera que la información concierne a una persona cuando se refiere a ella. 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.

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.**

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.

**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).**

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”. Art. 3° Fracc. **VII. Datos Personales**: La información concerniente a una persona física, identificada o identificable; **Ley de Transparencia QROO**

Modulo 2 **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.

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.

A partir de la segunda mitad del siglo XX se empiezan a producir una serie de avances científico-tecnológicos vertiginosos: 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.

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.

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.**

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.

 **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”.

**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**

En el ámbito del Consejo de Europa, se aprobó el Convenio No. 108, el 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 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.

**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

Ley de Protección de Datos Personales para el Distrito Federal (LPDPDF), que entra en vigor desde el 4 de octubre de 2008

“protección de datos personales” es la “la garantía que tutela la privacidad de datos personales en poder de los entes públicos”.

**Los derechos ARCO** (acceso, rectificación, cancelación y oposición) son el conjunto de **derechos** a través de los cuales la Ley Orgánica 15/1999 de **Protección de Datos de Carácter Personal (**Lopd) garantiza a las personas el poder de control sobre sus datos personales.

El derecho de acceso: Permite a las personas acudir a la autoridad para solicitarle información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad de este, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas por los mismos.

**Los Derechos de rectificación y cancelación**: se encuentran el artículo 6° constitucional, estas dos opciones de que dispone el ciudadano cuando sus datos sometidos por la autoridad resultan ser inexactos, incompletos, inadecuados o excesivos. En estos supuestos, el titular puede requerir a la autoridad que los rectifique y registre los que correspondan o bien que cancele sus datos y los elimine definitivamente del fichero.

**El derecho de oposición**: consiste en la facultad que posee el titular de los datos para dirigirse al responsable de la información y requerirle que deje de tratar sus datos personales cuando se están tratando sin su consentimiento, cuando se utilicen con fines de publicidad o comercial.

* Los derechos **ARCO** son personalísimos “Solo pueden ser ejercidos por el titular de los datos o por su representante legal, o quien tenga la guardia y custodia del titular.
* Derechos Independientes por esto no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio del otro.
* La autoridad es el sujeto obligado a respetar, garantizar, proteger y promover este derecho.

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. 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.

**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.**

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.

|  |  |
| --- | --- |
| **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. |
| 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 datospersonales 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. |

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.

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 que incorpora la LPDPDF (artículo 5):* Licitud.
* Consentimiento.
* Calidad de los datos.
* Confidencialidad.
* Seguridad.
* Disponibilidad.
* Temporalidad
 |

**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.

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.

|  |
| --- |
| 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).***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, no está permitido, salvo que sea para fines históricos, estadísticos o científicos. |

**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:

1. ***Cierto*:** Cuando los datos se mantienen actualizados, que no se altere la veracidad de la información, evitando que el titular se vea afectado.
2. ***Adecuado*:** Cuando se observa una relación proporcional entre los datos recabados y la finalidad del tratamiento.
3. ***Pertinente*:** Cuando es realizado por el personal autorizado para el cumplimiento de las atribuciones de los entes públicos que los hayan recabado.
4. ***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.

***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.***

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.

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**, consiste 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.

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**, 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.

**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 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.

**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. 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.
* 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.

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

**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.

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.

**Tema 4:**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.

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.

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.

“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 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, 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.

Esta determinación debe ser publicada en la Periódico oficial y es necesario incluir, en los casos de creación de sistemas de datos personales, al menos, los siguientes aspectos:

1. La finalidad del sistema de datos personales y los usos previstos para el mismo.
2. Las personas o grupos de personas sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.
3. El procedimiento de recolección de los datos de carácter personal.
4. La estructura básica del sistema de datos personales y la descripción de los tipos de datos incluidos en el mismo.
5. De la cesión de las que pueden ser objeto los datos.
6. Las instancias responsables del tratamiento del sistema de datos personales.
7. La unidad administrativa ante la que podrán ejercitarse los derechos de acceso, rectificación, cancelación u oposición.
8. El nivel de protección exigible.

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

**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.**

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”

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:

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.

Leyenda que deben utilizar los entes públicos para informar a los interesados de estas advertencias:

|  |
| --- |
| ***Ejemplo de texto en la Ciudad de México:*** ***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***](http://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.

Entonces las excepciones al deber de informar son:

* Que se haya informado al interesado con anterioridad.
* Que así lo prevea expresamente una Ley.
* Cuando los datos provengan de fuentes accesibles al público en general.
* 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.

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.

Datos de carácter personal obtenidos para fines policiales. Pueden ser recabados sin consentimiento pero 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 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**

**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.

**Obligaciones que deben ser observadas por los entes públicos en cuanto a las medidas de seguridad, mismas que deberán:**

* Responder al nivel de protección que ameriten los datos.
* Constar por escrito y **comunicar el nivel aplicable al Instituto para su registro**.
* Señalar nombre y cargo del servidor público responsable del sistema de datos personales.
* Especificar a la persona física o moral que intervenga como usuario e indicar datos del acto jurídico por el que se otorgó el tratamiento.
* 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:

* Documentos de seguridad.
* Funciones y obligaciones del personal que intervenga en el tratamiento de los sistemas de datos personales.
* Registro de incidencias.
* Identificación y autentificación.
* Control de acceso.
* Gestión de soportes.
* 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:

* Responsable de seguridad.
* Auditoría.
* Control de acceso físico.
* 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:

* + Distribución de soportes.
	+ Registro de acceso.
	+ Telecomunicaciones.

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

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.

*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:

1. La descripción del tipo de incidencia.
2. El momento en que se presentó.
3. Persona que realiza la notificación.
4. A quién se comunica.
5. 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 autorizado 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:

1. 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.
2. 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 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. 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. 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. |

**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.

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:

1. La identificación de quien accedió.
2. La fecha y hora.
3. El sistema accedido.
4. 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.

**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, que garanticen que la comunicación entre dos puntos es segura, y no pueda ser interceptada por terceras personas.

* 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.
* 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.
* 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.
* 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.
* 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 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.
* 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 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.***

* 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.
* 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.
* 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.

**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**

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:

* El que se haya establecido en el formato físico o electrónico por medio del cual se recabaron.
* El establecido por las disposiciones aplicables.
* El establecido en el instrumento jurídico formalizado entre un tercero y el ente público.

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:

* Nombre del ente público a quien se dirija.
* Nombre completo del interesado, en su caso, el de su representante legal.
* Descripción clara y precisa de los datos personales respecto de los que se pretende revocar el consentimiento.
* Cualquier otro elemento que facilite su localización.
* El domicilio, mismo que se debe encontrar dentro del Distrito Federal, o medio electrónico para recibir notificaciones.
* 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.

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 8. Instituto de Acceso a la Información Públicadel 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.

En el estado de Quintana Roo, el Instituto de Acceso a la Información Pública y Protección de Datos Personales IDAIPQROO, es el encargado de dirigir y vigilar el cumplimiento de la Ley de Protección a Datos Personales, así como de las normas que de ella deriven.

**Dentro de éstas destacan:**

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

**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.

*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  “Oficina de Información Pública (OIP) correspondiente:

* Por **escrito material**ante la OIP, o enviado por correo ordinario, certificado o mensajería.
* **Verbal**, de manera oral y directa, la cual será capturada por el responsable de la OIP en el formato respectivo e ingresado al sistema http://infomex.qroo.gob.mx/
* **Correo electrónico**a la dirección de correo electrónico asignada a la OIP.
* Por el sistema electrónico **INFOMEX-QROO**.
* Vía teléfono, **al 983 8350650 EXT. 34450,** a través del correo **transparencia.sgp@qroo.gob.mx****.**

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 aclares o corrijas las deficiencias que detectó. Si este es el caso, tendrás diez 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 diez 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.

Acceso, Rectificación,

Cancelación, Oposición

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.

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).

**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.**

**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 prevención tendrá el efecto de interrumpir el plazo que tienen los Organismos garantes para resolver el recurso, por lo que comenzará a computarse a partir del día siguiente a su desahogo.**

No podrá prevenirse por el nombre que proporcione y con el que se ostente el recurrente, salvo que no coincida con el del interesado que presentó la solicitud de información que motivó el Recurso de Revisión;

Oficina de Información Pública (OIP)

**Artículo 147 LGT.** En todo momento, los Comisionados deberán tener acceso a la información clasificada para determinar su naturaleza según se requiera. El acceso se dará de conformidad con la normatividad previamente establecida por los sujetos obligados para el resguardo o salvaguarda de la información.

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, 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.

* **Artículo 144.** El recurso de revisión deberá contener:
* I. El sujeto obligado ante la cual se presentó la solicitud;
* II. El nombre del solicitante que recurre o de su representante y, en su caso, del tercero interesado, así como la dirección o medio que señale para recibir notificaciones;
* III. El número de folio de respuesta de la solicitud de acceso;
* IV. La fecha en que fue notificada la respuesta al solicitante o tuvo conocimiento del acto reclamado, o de presentación de la solicitud, en caso de falta de respuesta;
* V. El acto que se recurre;
* VI. Las razones o motivos de inconformidad, y
* VII. La copia de la respuesta que se impugna y, en su caso, de la notificación correspondiente, salvo en el caso de respuesta de la solicitud.

Los “agravios” los podemos entender como la aplicación indebida de las disposiciones de la Ley de Protección de Datos Personales 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 \_\_\_\_\_\_\_\_ días, lo prevendrá para que en un periodo de cinco días hábiles corrija las irregularidades encontradas.

***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:
	+ Permita el acceso a los datos solicitados.
	+ Rectifique los datos.
	+ Cancele los datos.

Las resoluciones del Instituto son definitivas, inatacables, salvo a través del juicio de amparo— y obligatorias para los particulares y para los entes públicos.

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.

**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,* 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 el Periódico oficial.
* Incumplir con los principios, con las resoluciones del IDAIP o con la presentación del informe.
* Obtención fraudulenta o engañosa de datos; transmisiones indebidas (lucro).
* Obstaculizar inspección del IDAIP.
* 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. Con fundamento en el Artículo 195. Serán causas de sanción por incumplimiento de las obligaciones establecidas en la materia de la Ley Estatal.

 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**.

Acceso, Rectificación,

Cancelación, Oposición

Ahora bien, los titulares de los datos personales, cuentan con el derecho de recurrir ante el Instituto de Acceso a la Información Pública de QROO -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.

Acceso, Rectificación,

Cancelación, Oposición