

Instituto de Acceso a la Información Pública del Distrito Federal

Acuerdo mediante el cual se aprueban los Lineamientos para la Protección de Datos Personales en el Distrito Federal.

EL PLENO DEL INSTITUTO DE ACCESO A LA INFORMACIÓN PÚBLICA DEL DISTRITO FEDERAL, CON FUNDAMENTO EN LOS ARTÍCULOS 23 Y 24, FRACCIÓN I, DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES PARA EL DISTRITO FEDERAL, PUBLICA EL SIGUIENTE:

ACUERDO 547/SO/14-10/2009

ACUERDO MEDIANTE EL CUAL SE APRUEBAN LOS LINEAMIENTOS PARA LA PROTECCIÓN DE DATOS PERSONALES EN EL DISTRITO FEDERAL.

CONSIDERANDO

1. Que de conformidad con el artículo 63 de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal (LTAIPDF), el Instituto de Acceso a la Información Pública del Distrito Federal (INFODF) es un órgano autónomo del Distrito Federal, con personalidad jurídica propia y patrimonio propio, con autonomía presupuestaria, de operación y de decisión en materia de transparencia y acceso a la información pública, encargado de dirigir y vigilar el cumplimiento de la Ley en la materia y las normas que de ella deriven, así como de velar porque los principios de certeza, legalidad, independencia, imparcialidad y objetividad imperen en todas sus decisiones.
2. Que de acuerdo al artículo 71, fracciones VII, XLI y XLIV de dicho ordenamiento, es atribución del Pleno del INFODF emitir su Reglamento Interno, manuales y demás normas que faciliten su organización y funcionamiento, así como dictar todas aquellas medidas para el mejor funcionamiento del Instituto y las demás que se deriven de la Ley en la materia y otras disposiciones aplicables.
3. Que de conformidad con lo establecido en el artículo 23 de la Ley de Protección de Datos Personales para el Distrito Federal (LPDPDF), el INFODF es el órgano encargado de dirigir y vigilar el cumplimiento de la Ley en mención y las normas que de ella deriven, además de ser la autoridad encargada de garantizar la protección y el correcto tratamiento de datos personales. También velará porque los principios de licitud, consentimiento, calidad de los datos, confidencialidad, seguridad, disponibilidad y temporalidad rijan en los sistemas de datos personales en posesión de los entes públicos del Distrito Federal.
4. Que de conformidad con el artículo 24, fracción I, de la LPDPDF, el INFODF tiene como atribución la 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 en posesión de los entes públicos.
5. Que de conformidad con el artículo 12, fracciones I y IV, del Reglamento Interior del INFODF, le corresponde al Pleno del Instituto: determinar la forma y términos en que serán ejercidas las atribuciones que al Instituto le otorga la LTAIPDF y la LPDPDF, así como dictar los acuerdos y normatividad necesarios para ejercer las atribuciones previstas en las leyes en comento, en el Reglamento Interior, y demás normatividad aplicable.
6. Que así mismo, la LPDPDF define como 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.”
7. Que existen datos personales en posesión de los entes públicos, los cuales fueron obtenidos en el marco de sus respectivas atribuciones, para determinados fines, y que a su vez son integrados a su correspondiente sistema de datos

personales. Este último, es definido por la LPDPDF como “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.”

8. Que todo dato personal es confidencial y por consiguiente deberá de ser protegido conforme a la LPDPDF. Motivo por el cual, los entes públicos deberán de llevar a cabo las medidas de seguridad para la protección de los sistemas de datos personales, y conducirse conforme los procedimientos y normas establecidas para el acceso, rectificación, cancelación y oposición de datos personales (ARCO).
9. Que atendiendo a las atribuciones con que cuenta el INFODF y a fin de fortalecer el marco normativo en materia de datos personales, el Instituto elaboró un proyecto de Lineamientos para la Protección de Datos Personales en el Distrito Federal, los cuales fueron analizados y fortalecidos con los comentarios y sugerencias de los entes públicos.
10. Que dicho proyecto de Lineamientos 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.
11. Que para tal efecto, el proyecto de Lineamientos en comento en su título primero establece definiciones de conceptos, aunque no limitativos, del derecho de la protección de datos personales; en su segundo título, 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; el tercer título, señala las atribuciones con que cuenta el INFODF para garantizar el cumplimiento de la LPDPDF por parte de los entes públicos, y el cuarto título, establece el procedimiento que deberán sujetarse tanto particulares como los sujetos obligados en el ejercicio del derecho ARCO.
12. Que de conformidad con el artículo 13, fracción IV del Reglamento Interior del INFODF, el Presidente tiene la facultad de someter a la aprobación del Pleno, a propuesta propia o de cualquier otro Comisionado, las normas, lineamientos y demás documentos necesarios para el cumplimiento de las atribuciones del Instituto.
13. Que en virtud de las consideraciones vertidas y en ejercicio de sus atribuciones, el Comisionado Ciudadano Presidente del INFODF somete a la consideración del Pleno, el **Proyecto de acuerdo mediante el cual se aprueban los Lineamientos para la Protección de Datos Personales en el Distrito Federal.**

Por las consideraciones y fundamentos anteriormente expuestos, el Pleno del Instituto de Acceso a la Información Pública del Distrito Federal emite el siguiente:

ACUERDO

PRIMERO. Se aprueban los Lineamientos para la Protección de Datos Personales en el Distrito Federal, **conforme al documento que, como anexo, forma parte del presente Acuerdo.**

SEGUNDO. El presente Acuerdo entrará en vigor el día siguiente de su publicación en la Gaceta Oficial del Distrito Federal.

TERCERO. El Presente Acuerdo deberá ser comunicado por el Presidente de este Instituto a los titulares de los entes públicos.

CUARTO. Se instruye al Secretario Técnico para que, en el ámbito de sus atribuciones, realice las acciones necesarias para publicar el presente acuerdo en la Gaceta Oficial del Distrito Federal, y en el portal de Internet del INFODF, así como para comunicarlo a los responsables de las Oficinas de Información Pública y a los Responsables de los Sistemas de Protección de Datos Personales designados por los titulares de los entes públicos del Distrito Federal.

Así lo acordó, por unanimidad, el Pleno del Instituto de Acceso a la Información Pública del Distrito Federal, en Sesión Ordinaria celebrada el catorce de octubre de dos mil nueve.

(Firma)

Oscar Mauricio Guerra Ford
Comisionado Ciudadano Presidente

(Firma)

Jorge Bustillos Roqueñí
Comisionado Ciudadano

(Firma)

Areli Cano Guadiana
Comisionada Ciudadana

(Firma)

Salvador Guerrero Chiprés
Comisionado Ciudadano

(Firma)

Agustín Millán Gómez
Comisionado Ciudadano

LINEAMIENTOS PARA LA PROTECCIÓN DE DATOS PERSONALES EN EL DISTRITO FEDERAL

TÍTULO PRIMERO. DISPOSICIONES COMUNES PARA LOS ENTES PÚBLICOS

CAPÍTULO ÚNICO. DISPOSICIONES GENERALES

TÍTULO SEGUNDO. DE LA TUTELA DE DATOS PERSONALES

CAPÍTULO I. DE LOS SISTEMAS DE DATOS PERSONALES

CAPÍTULO II. DE LAS MEDIDAS DE SEGURIDAD

CAPÍTULO III. DEL TRATAMIENTO DE DATOS PERSONALES

CAPÍTULO IV. DE LAS OBLIGACIONES DE LOS ENTES PÚBLICOS

TÍTULO TERCERO. DE LA AUTORIDAD RESPONSABLE DEL CONTROL Y VIGILANCIA

CAPÍTULO ÚNICO. INSTITUTO DE ACCESO A LA INFORMACIÓN PÚBLICA DEL DISTRITO FEDERAL

TÍTULO CUARTO. DE LOS DERECHOS Y DEL PROCEDIMIENTO PARA SU EJERCICIO

CAPÍTULO ÚNICO. DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN.

TRANSITORIOS

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:

- I. Autenticación: Comprobación de la identidad de aquella persona autorizada para el tratamiento de datos personales;
- II. 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;
- III. Cancelación: Eliminación de determinados datos de un sistema de datos personales previo bloqueo de los mismos;
- IV. Cesionario: Persona física o moral, pública o privada, a la que un ente público realice una cesión de datos personales;

- V. 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;
- VI. 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;
- VII. Encargado: Servidor público que en ejercicio de sus atribuciones, realiza tratamiento de datos personales de forma cotidiana;
- VIII. 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;
- IX. 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;
- X. Incidencia: Cualquier anomalía que afecte o pudiera afectar la seguridad de los datos personales;
- XI. 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;
- XII. 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;
- XIII. Lineamientos: Lineamientos para la Protección de Datos Personales en el Distrito Federal;
- XIV. Ley: Ley de Protección de Datos Personales para el Distrito Federal;
- XV. 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;
- XVI. 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;
- XVII. 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;
- XVIII. 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;
- XIX. 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;
- XX. 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;
- XXI. Supresión: Eliminación de un sistema de datos personales mediante acuerdo publicado en la Gaceta Oficial del Distrito Federal; y
- XXII. 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:

- I. 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
- II. Automatizados: Conjunto ordenado de datos de carácter personal que permita acceder a la información relativa a una persona física utilizando 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:

- I. 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;
- II. 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;
- III. Datos laborales: Documentos de reclutamiento y selección, nombramiento, incidencia, capacitación, actividades extracurriculares, referencias laborales, referencias personales, solicitud de empleo, hoja de servicio, demás análogos;
- IV. 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;
- V. 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;
- VI. Datos académicos: Trayectoria educativa, calificaciones, títulos, cédula profesional, certificados y reconocimientos, demás análogos;
- VII. Datos de tránsito y movimientos migratorios: Información relativa al tránsito de las personas dentro y fuera del país, así como información migratoria;
- VIII. 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;
- IX. Datos biométricos: huellas dactilares, ADN, geometría de la mano, características de iris y retina, demás análogos;
- X. Datos especialmente protegidos (sensibles): origen étnico o racial, características morales o emocionales, ideología y opiniones políticas, creencias, convicciones religiosas, filosóficas y preferencia sexual; y
- XI. 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:

- I. La identificación del sistema de datos personales, indicando su denominación y normativa aplicable, así como la descripción de la finalidad y usos previstos;
- 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);

- III. 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;
- IV. Las cesiones de datos que se tengan previstas, indicando, en su caso, los destinatarios o categorías de destinatarios;
- V. La identificación de la unidad administrativa a la que corresponde el sistema de datos personales, así como del cargo del responsable;
- VI. 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
- VII. 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:

- I. Nombre del Sistema y, en su caso, fecha de publicación en la Gaceta Oficial del Distrito Federal;
- II. Nombre y cargo del responsable del sistema;
- III. Finalidades y usos previstos, así como el soporte en el que se encuentra;
- IV. La categoría de los datos personales contenidos en el sistema, forma de recolección y actualización de los mismos;
- V. Unidad administrativa en la que se encuentra el sistema;
- VI. Destino y personas físicas o morales a las que puedan ser transmitidos;
- VII. Modo de interrelacionar la información contenida en el sistema y el plazo de conservación de los datos;
- VIII. Teléfono y correo electrónico del responsable;
- IX. Normativa aplicable al sistema; e
- X. 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 deber 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:

- I. Nombre del sistema;
- II. Cargo y adscripción del responsable;
- III. Ámbito de aplicación;
- IV. Estructura y descripción del sistema de datos personales;
- V. Especificación detallada de la categoría de datos personales contenidos en el sistema;

- VI. Funciones y obligaciones del personal que intervenga en el tratamiento de los sistemas de datos personales;
- VII. Medidas, normas, procedimientos y criterios enfocados a garantizar el nivel de seguridad exigido por el artículo 14 de la Ley y los presentes Lineamientos;
- VIII. Procedimientos de notificación, gestión y respuesta ante incidencias;
- IX. Procedimientos para la realización de copias de respaldo y recuperación de los datos, para los sistemas de datos personales automatizados; y
- X. 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 autenticación

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 permitirse 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:

- a) Libre: Cuando es obtenido sin la intervención de vicio alguno de la voluntad;
- b) Inequívoco: Cuando existe expresamente una acción que implique su otorgamiento;
- c) Específico: Cuando se otorga referido a una determinada finalidad; e
- d) 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:

- a) 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;
- 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; e
- 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.

IV. Con relación al principio de confidencialidad, se entenderá que los datos personales son:

- a) Irrenunciables: El interesado está imposibilitado de privarse voluntariamente de las garantías que le otorga la legislación en materia de protección de datos personales;
- b) Intransferibles: El interesado es el único titular de los datos y éstos no pueden ser cedidos a otra persona; e
- c) 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:

- I. 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;
- II. Requerir al responsable la cancelación o rectificación de determinados datos contenidos en el sistema que corresponda;
- III. Requerir que el responsable modifique el sistema a efecto de que se ajuste a lo establecido en la Ley y demás normativa aplicable; y
- IV. 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 exigirse 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:

- I. El que se haya establecido en el formato físico o electrónico por medio del cual se recabaron;
- II. El establecido por las disposiciones aplicables; y
- III. 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:

- I. Número de solicitudes de acceso, rectificación, cancelación y oposición de datos personales presentadas ante el ente público, así como su resultado;
- II. El tiempo de respuesta a la solicitud;
- III. El estado que guardan las denuncias presentadas ante los órganos internos de control, así como de las vistas dadas por el Instituto;
- IV. Dificultades observadas en el cumplimiento de la Ley;
- V. Descripción de los recursos públicos utilizados en la materia;
- VI. Sistemas de datos personales creados, modificados y/o suprimidos;
- VII. Acciones desarrolladas para dar cumplimiento a las disposiciones contenidas en la Ley; y
- VIII. Cesiones de datos personales efectuadas que deberá detallar:
 - a) Identificación del sistema mediante número de folio otorgado por el Instituto, del ente cedente y del cesionario;
 - b) Finalidad de la cesión;
 - c) 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;
 - d) Fecha de inicio y término de la cesión y, en su caso, la periodicidad de la misma;
 - e) Medio empleado para realizar la cesión;
 - f) Medidas y niveles de seguridad empleados para la cesión;
 - g) Obligaciones al término del tratamiento; y
 - h) El nivel de seguridad aplicado por el cesionario.

Enlace

38. El servidor público designado como enlace tendrá las siguientes obligaciones:

- I. 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;
- II. Supervisar que los responsables mantengan actualizada la inscripción de los sistemas bajo su responsabilidad en el Registro electrónico creado por el Instituto;
- III. Coordinar las acciones en materia de capacitación; y
- IV. 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:

- I. Toda visita de inspección deberá ajustarse a los procedimientos y formalidades establecidos en estos Lineamientos;
- II. 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;
- III. 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;
- IV. 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;
- V. 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;
- VI. 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;
- VII. En las actas se hará constar:
 - a) Identificación del ente público visitado;
 - b) Hora, día, mes y año en que se inicie y concluya la diligencia;
 - c) 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;
 - d) Número y fecha del acuerdo del Pleno que la motivó;
 - e) Nombre y cargo de la persona con quien se entendió la diligencia;
 - f) Nombre y cargo de las personas que fungieron como testigos;
 - g) Datos relativos a la actuación;
 - h) Declaración del visitado, si quiere hacerla; y
 - i) 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.
- VIII. 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;
- IX. 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
- X. 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:
 - a) Determinar que el sistema de datos personales se ajusta a lo establecido en la Ley;
 - b) 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;
 - c) 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

- d) 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 rectificadas 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.

CUARTO. Los entes públicos contarán con ciento veinte días hábiles para realizar las adecuaciones necesarias que permitan atender los requerimientos sobre las medidas de seguridad referidas en estos Lineamientos.
