INSTITUTO FEDERAL DE ACCESO A LA INFORMACION PUBLICA

LINEAMIENTOS de Protección de Datos Personales.

Al margen un sello con el Escudo Nacional, que dice: Estados Unidos Mexicanos.- Instituto Federal de Acceso a la Información Pública.

El Pleno del Instituto Federal de Acceso a la Información Pública, con fundamento en lo dispuesto por los artículos 37 fracción IX de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, y 2 fracción III, 47 y 62 fracciones I y II de su Reglamento, y:

Reconociendo que el respeto a la dignidad de la persona es un valor central de los Estados democráticos que tienen como fundamento la búsqueda de la justicia, la libertad, la igualdad, la seguridad y la solidaridad, y que es a partir de la afirmación de dicha dignidad que existen y se legitiman todos los derechos;

Considerando que en nuestro país, fue voluntad del legislador plasmar en la Constitución Política de los Estados Unidos Mexicanos el derecho a la *vida privada* también denominada por la doctrina *intimidad,* como límite a la intromisión del Estado en el ámbito de la persona, al plasmar en su artículo 16 que: "nadie puede ser molestado *en su persona, familia, domicilio, papeles o posesiones*, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento", por lo que el derecho a la intimidad tiene dos facetas principales: una que tutela la inviolabilidad del hogar, de las comunicaciones y de las relaciones familiares, y otra que consagra el derecho del individuo a desarrollarse libremente como tal;

Observando que los artículos 6o. y 7o. Constitucionales establecen como límite a la manifestación de las ideas y a la libertad de imprenta respectivamente, el ataque a los derechos de tercero y el *respeto a la vida privada*, la libertad de expresar o publicar pensamientos encuentra entonces una restricción *cuando con ello se menoscabe a la persona.* Asimismo, el artículo 6o. consagra el derecho a la información, el cual será garantizado por el Estado, que para efectos de la regulación que en el presente instrumento se emite, se interpreta como el derecho del individuo a tener acceso a la información sobre sí mismo que obra en bancos de datos y a que sus datos no sean manejados de manera indebida;

Reconociendo que a nivel internacional se configura la existencia del derecho humano a la vida privada, por el cual: "ninguna persona puede ser objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación, gozando del derecho a la protección de la ley contra tales injerencias o ataques". Lo anterior se establece en los siguientes instrumentos internacionales, los cuales por virtud del artículo 133 Constitucional constituyen Ley Suprema de la Unión: la Declaración Universal de los Derechos Humanos –artículo 12-; el Pacto Internacional de Derechos Civiles y Políticos -artículo 17-; la Declaración Americana de los Derechos y Deberes del Hombre -artículo V-; la Convención Americana sobre Derechos Humanos -artículo 11-, y la Convención sobre los Derechos del Niño -artículo 16-;

Recordando que en el marco jurídico vigente en México existen diversas disposiciones que regulan las consecuencias de los ataques o invasiones a la vida privada de las personas en el orden administrativo, civil, penal y de responsabilidad patrimonial del Estado, por lo que existe un acervo jurídico que brinda protección al individuo frente a injerencias ilegales en su vida privada;

Admitiendo que la sociedad de la información, fundada en el avance vertiginoso de la tecnología, ofrece al individuo ventajas diversas que contribuyen a mejorar su calidad de vida y, en el caso del Estado, a mejorar la actividad administrativa, el desarrollo económico, social y cultural, así como el cumplimiento de las obligaciones ciudadanas frente a éste, pero que, al mismo tiempo, una mala utilización de las herramientas tecnológicas puede convertirse en un factor de amenaza a la privacidad y seguridad de las personas al permitir que se generen formas de exclusión o condiciones de incertidumbre y riesgo, ya que las nuevas tecnologías facilitan ilimitadas posibilidades para mover un gran volumen de información y de interrelacionarla, de manera que se constituyen perfiles que pueden limitar la libertad o condicionar el modo de actuar de las personas;

Reconociendo que como consecuencia de lo anterior, y a efecto de lograr un uso racional y ético de las tecnologías, en el concierto de las naciones se ha legislado en materia de protección de datos personales, por lo cual los individuos gozan de un nuevo derecho denominado a la autodeterminación informativa, como garantía del ciudadano en las modernas sociedades frente al desafío del tratamiento electrónico de sus datos, entendida la garantía como la facultad del individuo de decidir quién, cuándo y bajo qué circunstancias utiliza sus datos personales, tanto en el sector público como en el privado;

Atendiendo a la evolución que ha ocurrido de la noción tradicional de intimidad o vida privada limitada al derecho de impedir interferencias ajenas, o al derecho a ser dejado solo, hasta el derecho de mantener el control de la propia información y de determinar la forma de construcción de la propia esfera privada, por lo que el derecho a la protección de los datos personales se presenta como un elemento esencial para el libre desarrollo de la persona en las sociedades democráticas;

Tomando en cuenta que la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental es obligatoria únicamente para los poderes públicos del Estado Federal, y tiene como uno de sus objetivos el de garantizar la protección de los datos personales en posesión de los sujetos obligados, así como el acceso y la corrección de los mismos por parte de sus titulares, estableciendo autoridades encargadas de dicha protección en cada sujeto obligado;

Reconociendo que el ejercicio de las atribuciones de las dependencias y entidades de la Administración Pública Federal implica recabar datos personales para los fines establecidos en las disposiciones aplicables, por lo que los servidores públicos deben ser los primeros obligados al cumplimiento de la Ley para promover el uso responsable de las nuevas tecnologías de la información, atendiendo los principios de protección de datos personales de licitud, calidad, de información al titular sobre el uso y destino de su información, de seguridad, custodia y consentimiento para su transmisión; principios que no limitan la utilización de la informática en el ámbito público, sino que se trata de hacerla compatible con los derechos de los ciudadanos;

Distinguiendo la importancia de que las personas tengan conocimiento de la información que de ellos obra en los archivos del Gobierno Federal a efecto de hacer uso del derecho de acceso y corrección de los datos personales que les conciernen, así como de conocer las transferencias de sistemas de datos personales efectuadas para el cumplimiento de las atribuciones de las unidades administrativas que lo conforman, se creará un nueva aplicación informática de acceso al público denominada “Sistema Persona”;

Considerando que la Administración Pública Federal debe proteger rigurosamente los datos personales, apegándose en forma escrupulosa a la regulación en la materia, sin que ello se constituya en pretexto u obstáculo que menoscabe el Estado de Derecho o impida el acceso a la información gubernamental y la rendición de cuentas, de manera que los ciudadanos puedan valorar el desempeño de los sujetos obligados por la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, por lo que ante una solicitud de acceso a información gubernamental en la que se requieran datos personales contenidos en un Sistema de datos personales, en cada caso, las dependencias y entidades deberán determinar la procedencia de otorgar acceso a aquellos datos que no se consideran como confidenciales, por ubicarse en los supuestos establecidos por los artículos 7, 12 y 18 último párrafo de dicha Ley, y

Resaltando que en el ámbito del Poder Ejecutivo Federal, el Instituto Federal de Acceso a la Información Pública es el garante de la protección de las personas respecto del tratamiento dado a la información que les concierne, a efecto de evitar injerencias a su vida privada, y que los principios contenidos en el capítulo IV del Título I de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental requieren de un desarrollo para su adecuada observancia, ha tenido a bien expedir los siguientes:

LINEAMIENTOS DE PROTECCION DE DATOS PERSONALES

Capítulo I
Disposiciones generales

Objeto y ámbito de aplicación

Primero. Los presentes Lineamientos tienen por objeto establecer las políticas generales y procedimientos que deberán observar las dependencias y entidades de la Administración Pública Federal para garantizar a la persona la facultad de decisión sobre el uso y destino de sus datos personales, con el propósito de asegurar su adecuado tratamiento e impedir su transmisión ilícita y lesiva para la dignidad y derechos del afectado.

Para tal efecto, este ordenamiento establece las condiciones y requisitos mínimos para el debido manejo y custodia de los sistemas de datos que se encuentren en posesión de la Administración Pública Federal en el ejercicio de sus atribuciones.

Elementos de los datos personales

Segundo. A efecto de determinar si la información que posee una dependencia o entidad constituye un dato personal, deberán agotarse las siguientes condiciones:

1) Que la misma sea concerniente a una persona física, identificada o identificable, y
2) Que la información se encuentre contenida en sus archivos.

Definiciones

Tercero. Para efectos de la aplicación de los presentes Lineamientos, además de las definiciones establecidas en los artículos 3 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, 2 de su Reglamento, y las referidas en los Lineamientos expedidos por el Instituto, publicados en el Diario Oficial de la Federación el 25 de agosto de 2003 y 6 de abril de 2004, se entenderá por:

I. Destinatario: Cualquier persona física o moral pública o privada que recibe datos personales.

II. Encargado: El servidor público o cualquier otra persona física o moral facultado por un instrumento jurídico o expresamente autorizado por el Responsable para llevar a cabo el tratamiento físico o automatizado de los datos personales.

III. Sistema "Persona": Aplicación informática desarrollada por el Instituto para mantener actualizado el listado de los sistemas de datos personales que posean las dependencias y entidades para registrar e informar sobre las transmisiones, modificaciones y cancelaciones de los mismos.

IV. Responsable: El servidor público titular de la unidad administrativa designado por el titular de la dependencia o entidad, que decide sobre el tratamiento físico o automatizado de datos personales, así como el contenido y finalidad de los sistemas de datos personales.

V. Titular de los datos: Persona física a quien se refieren los datos personales que sean objeto de tratamiento.

VI. Transmisión: Toda entrega total o parcial de sistemas de datos personales realizada por las dependencias y entidades a cualquier persona distinta al Titular de los datos, mediante el uso de medios físicos o electrónicos tales como la interconexión de computadoras, interconexión de bases de datos, acceso a redes de telecomunicación, así como a través de la utilización de cualquier otra tecnología que lo permita.

VII. Transmisor: Dependencia o entidad que posee los datos personales objeto de la transmisión.

VIII. Tratamiento: Operaciones y procedimientos físicos o automatizados que permitan recabar, registrar, reproducir, conservar, organizar, modificar, transmitir y cancelar datos personales.

IX. Usuario: Servidor público facultado por un instrumento jurídico o expresamente autorizado por el Responsable que utiliza de manera cotidiana datos personales para el ejercicio de sus atribuciones, por lo que accede a los sistemas de datos personales, sin posibilidad de agregar o modificar su contenido.

Sistema de datos personales

Cuarto. Un Sistema de datos personales constituye el conjunto ordenado de datos personales que estén en posesión de una dependencia o entidad, con independencia de su forma de acceso, creación, almacenamiento u organización.

Los sistemas de datos personales podrán distinguirse entre físicos y automatizados, definiéndose cada uno de ellos de la siguiente forma:

a) Físicos: Conjunto ordenado de datos que para su tratamiento están contenidos en registros manuales, impresos, sonoros, magnéticos, visuales u holográficos.

b) Automatizados: Conjunto ordenado de datos que para su tratamiento han sido o están sujetos a un tratamiento informático y que por ende requieren de una herramienta tecnológica específica para su acceso, recuperación o tratamiento.

Capítulo II
Principios rectores de la Protección de los Datos Personales

Principios de la protección de datos personales

Quinto. En el tratamiento de datos personales, las dependencias y entidades deberán observar los principios de licitud, calidad, acceso y corrección, de información, seguridad, custodia y consentimiento para su transmisión.

Licitud

Sexto. La posesión de sistemas de datos personales deberá obedecer exclusivamente a las atribuciones legales o reglamentarias de cada dependencia o entidad y deberán obtenerse a través de los medios previstos en dichas disposiciones.

Los datos personales deberán tratarse únicamente para la finalidad para la cual fueron obtenidos. Dicha finalidad debe ser determinada y legítima.

Calidad de los datos

Séptimo. El tratamiento de datos personales deberá ser exacto, adecuado, pertinente y no excesivo, respecto de las atribuciones legales de la dependencia o entidad que los posea.

Acceso y corrección

Octavo. Los sistemas de datos personales deberán almacenarse de forma tal que permitan el ejercicio de los derechos de acceso y corrección previstos por la Ley, el Reglamento y los Lineamientos emitidos por el Instituto.

De Información

Noveno. Se deberá hacer del conocimiento del Titular de los datos, al momento de recabarlos y de forma escrita, el fundamento y motivo de ello, así como los propósitos para los cuales se tratarán dichos datos.

Seguridad

Décimo. Se deberán adoptar las medidas necesarias para garantizar la integridad, confiabilidad, confidencialidad y disponibilidad de los datos personales mediante acciones que eviten su alteración, pérdida, transmisión y acceso no autorizado.

Custodia y cuidado de la información

Undécimo. Los datos personales serán debidamente custodiados y los Responsables, Encargados y Usuarios deberán garantizar el manejo cuidadoso en su tratamiento.

Consentimiento para la transmisión

Duodécimo. Toda transmisión de datos personales deberá contar con el consentimiento del Titular de los datos, mismo que deberá otorgarse en forma libre, expresa e informada, salvo lo dispuesto en el Lineamiento Vigésimo segundo.

Capítulo III
Del Tratamiento

Tratamiento exacto, adecuado, pertinente y no excesivo

Decimotercero. A efecto de cumplir con el principio de calidad a que se refiere el Lineamiento Séptimo, se considera que el tratamiento de datos personales es:

a) Exacto: Cuando los datos personales se mantienen actualizados de manera tal que no altere la veracidad de la información que traiga como consecuencia que el Titular de los datos se vea afectado por dicha situación;

b) Adecuado: Cuando se observan las medidas de seguridad aplicables;

c) Pertinente: Cuando es realizado por el personal autorizado para el cumplimiento de las atribuciones de las dependencias y entidades que los hayan recabado, y

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

Corrección de oficio

Decimocuarto. En caso de que los Responsables, Encargados o Usuarios detecten que hay datos personales inexactos, deberán de oficio, actualizarlos en el momento en que tengan conocimiento de la inexactitud de los mismos, siempre que posean los documentos que justifiquen la actualización.

Conservación de los datos

Decimoquinto. Los datos personales que hayan sido objeto de tratamiento y no contengan valores históricos, científicos, estadísticos o contables, deberán ser dados de baja por las dependencias y entidades, o bien, los que contengan dichos valores serán objeto de transferencias secundarias, de conformidad con lo establecido por los catálogos de disposición documental a que se refieren los Lineamientos Generales para la organización y conservación de archivos de las Dependencias y Entidades de la Administración Pública Federal, teniendo en cuenta los siguientes plazos:

a) El que se haya establecido en el formato físico o electrónico por el cual se recabaron;
b) El establecido por las disposiciones aplicables;
c) El establecido en los convenios formalizados entre una persona y la dependencia o entidad, y
d) El señalado en los casos de transmisión.

Condiciones técnicas

Decimosexto. Los datos personales sólo podrán ser tratados en sistemas de datos personales que reúnan las condiciones de seguridad establecidas en los presentes Lineamientos y las demás disposiciones aplicables.

Información al Titular de los datos

Decimoséptimo. En el momento en que se recaben datos personales, la dependencia o entidad deberá hacer del conocimiento al Titular de los datos tanto en los formatos físicos como en los electrónicos utilizados para ese fin, lo siguiente:

a) La mención de que los datos recabados serán protegidos en términos de lo dispuesto por la Ley;
b) El fundamento legal para ello, y
c) La finalidad del Sistema de datos personales.

Modelo de leyenda para informar al Titular de los datos

Decimoctavo. Sin perjuicio de que las dependencias y entidades elaboren sus propios formatos para informar al Titular de los datos lo establecido por el Lineamiento anterior, podrán utilizar el siguiente modelo:

Los datos personales recabados serán protegidos y serán incorporados y tratados en el Sistema de datos personales (indicar nombre[1]), con fundamento en (indicar [2]) y cuya finalidad es (describirla[3]), el cual fue registrado en el Listado de sistemas de datos personales ante el Instituto Federal de Acceso a la Información Pública (www.ifai.org.mx), y podrán ser transmitidos a (indicar [4]), con la finalidad de (indicar [5]), además de otras transmisiones previstas en la Ley. La Unidad Administrativa responsable del Sistema de datos personales es (indicarlo[6]), y la dirección donde el interesado podrá ejercer los derechos de acceso y corrección ante la misma es (indicarla[7]). Lo anterior se informa en cumplimiento del Decimoséptimo de los Lineamientos de Protección de Datos Personales, publicados en el Diario Oficial de la Federación (incluir fecha[8]).

Otros medios para recabar los datos

Decimonoveno. Las dependencias y entidades que recaben datos personales a través de un servicio de orientación telefónica, u otros medios o sistemas, deberán establecer un mecanismo por el que se informe previamente a los particulares que sus datos personales serán recabados, la finalidad de dicho acto así como el tratamiento al cual serán sometidos, cumpliendo con lo establecido en el Decimoséptimo de los presentes Lineamientos.

Disociación de datos

Vigésimo. La disociación consiste en el procedimiento por el cual los datos personales no pueden asociarse al Titular de éstos, ni permitir por su estructura, contenido o grado de desagregación, la identificación individual del mismo.

El tratamiento de datos personales para fines estadísticos deberá efectuarse mediante la disociación de los datos, de conformidad con la Ley de Información Estadística y Geográfica, así como las demás disposiciones aplicables.

Tratamiento de datos por terceros

Vigésimo primero. Cuando se contrate a terceros para que realicen el tratamiento de datos personales, deberá estipularse en el contrato respectivo, la implementación de medidas de seguridad y custodia previstas en los presentes Lineamientos, en la normatividad aplicable a las dependencias y entidades contratantes, así como la imposición de penas convencionales por su incumplimiento.

Capítulo IV
De la transmisión

Transmisión sin consentimiento del Titular de los datos

Vigésimo segundo. Las dependencias y entidades podrán transmitir datos personales sin el consentimiento del Titular de los datos, en los casos previstos en el artículo 22 de la Ley. Asimismo, deberán otorgar acceso a aquellos datos que no se consideran como confidenciales por ubicarse en los supuestos establecidos por sus artículos 7, 12 y 18 último párrafo.

Transmisión con el consentimiento del Titular de los datos

Vigésimo tercero. Para los efectos del artículo 21 de la Ley, y en los casos no previstos por el artículo 22 de la Ley, las dependencias y entidades sólo podrán transmitir datos personales cuando:

a) Así lo prevea de manera expresa una disposición legal, y
b) Medie el consentimiento expreso de los titulares.

Consentimiento

Vigésimo cuarto. Para la transmisión de los datos, el consentimiento del Titular de los mismos deberá otorgarse por escrito incluyendo la firma autógrafa y la copia de identificación oficial, o bien a través de un medio de autenticación. En su caso, las dependencias y entidades deberán cumplir con las disposiciones aplicables en materia de certificados digitales y/o firmas electrónicas.

El servidor público encargado de recabar el consentimiento del Titular de los datos para la transmisión de los mismos, deberá entregar a éste, en forma previa a cada transmisión, la información suficiente acerca de las implicaciones de otorgar, de ser el caso, su consentimiento.

Informes sobre la transmisión

Vigésimo quinto. Las transmisiones totales o parciales de sistemas de datos personales que realicen las dependencias y entidades en el ejercicio de sus atribuciones, deberán ser notificadas por el Responsable al Instituto en los términos establecidos por el Cuadragésimo de los presentes Lineamientos.

---

1 Indicar el nombre del sistema de datos personales.
2 Indicar el fundamento legal que faculta a la dependencia o entidad para recabar los datos personales en el sistema de datos personales.
3 Describir la finalidad del sistema de datos personales.
4 Indicar las personas u organismos a los que podrán transmitirse los datos personales contenidos en el sistema de datos personales.
5 Describir la finalidad de la transmisión.
6 Indicar el nombre de la unidad administrativa responsable del sistema de datos personales.
7 Indicar la dirección de la unidad de enlace de la dependencia o entidad que posee el sistema de datos personales.
8 Anotar la fecha de publicación en el Diario Oficial de la Federación de los presentes Lineamientos.

Requisitos del Informe

Vigésimo sexto. El informe a que hace referencia el Lineamiento anterior deberá contener al menos, lo siguiente:

I. Identificación del Sistema de datos personales, del transmisor y del destinatario de los datos;

II. Finalidad de la transmisión; así como el tipo de datos que son objeto de la transmisión;

III. Las medidas de seguridad y custodia que adoptaron o fueron adoptadas por el transmisor y destinatario;

IV. Plazo por el que conservará el destinatario los datos que le hayan sido transmitidos, el cual podrá ser ampliado mediante aviso al Instituto, y

V. Señalar si una vez concluidos los propósitos de la transmisión, los datos personales deberán ser destruidos o devueltos al transmisor, al igual que cualquier soporte o documento en que conste algún dato de carácter personal objeto de la transmisión.

Capítulo V
De la Seguridad de los Sistemas de Datos Personales

Medidas de seguridad

Vigésimo séptimo. Para proveer seguridad a los sistemas de datos personales, los titulares de las dependencias y entidades deberán adoptar las medidas siguientes:

I. Designar a los Responsables;

II. Proponer al Comité de Información, la emisión de criterios específicos sobre el manejo, mantenimiento, seguridad y protección de los sistemas de datos personales, los cuales no podrán contravenir lo dispuesto por los presentes Lineamientos;

III. Proponer al Comité la difusión de la normatividad entre el personal involucrado en el manejo de los sistemas de datos personales, y

IV. Proponer al Comité la elaboración de un plan de capacitación en materia de seguridad de datos personales dirigida a los Responsables, Encargados y Usuarios.

Acciones sobre seguridad

Vigésimo octavo. En cada dependencia o entidad, el Comité coordinará y supervisará las acciones de promoción del manejo, mantenimiento, seguridad y protección de los sistemas de datos personales, así como de la integridad, confiabilidad, disponibilidad y exactitud de la información contenida en dichos sistemas de datos personales.

Reserva de la información

Vigésimo noveno. La documentación generada para la implementación, administración y seguimiento de las medidas de seguridad administrativa, física y técnica tendrá el carácter de información reservada y será de acceso restringido.

El personal que tenga acceso a dicha documentación deberá evitar que ésta sea divulgada, a efecto de no comprometer la integridad, confiabilidad, confidencialidad y disponibilidad de los sistemas de datos personales así como del contenido de éstos.

Resguardo de sistemas de datos personales físicos

Trigésimo. El Responsable deberá:

a) Adoptar las medidas para el resguardo de los sistemas de datos personales en soporte físico, de manera que se evite su alteración, pérdida o acceso no autorizado;

b) Autorizar expresamente, en los casos en que no esté previsto por un instrumento jurídico, a Encargados y Usuarios, y llevar una relación actualizada de las personas que tengan acceso a los sistemas de datos personales que se encuentran en soporte físico, y

c) Informar al Comité los nombres de los Encargados y Usuarios.

Sitio seguro para sistemas de datos personales automatizados

Trigésimo primero. Las dependencias y entidades deberán:

I. Asignar un espacio seguro y adecuado para la operación de los sistemas de datos personales;

II. Controlar el acceso físico a las instalaciones donde se encuentra el equipamiento que soporta la operación de los sistemas de datos personales debiendo registrarse para ello en una bitácora;

III. Contar con al menos dos lugares distintos, que cumplan con las condiciones de seguridad especificadas en estos Lineamientos, destinados a almacenar medios de respaldo de sistemas de datos personales;

IV. Realizar procedimientos de control, registro de asignación y baja de los equipos de cómputo a los Usuarios que utilizan datos personales, considerando al menos las siguientes actividades:

a) Si es asignación, configurarlo con las medidas de seguridad necesarias, tanto a nivel operativo como de Infraestructura, y

b) Verificar y llevar un registro del contenido del equipo para facilitar los reportes del Usuario que lo recibe o lo entrega para su baja.

V. Implantar procedimientos para el control de asignación y renovación de claves de acceso a equipos de cómputo y a los sistemas de datos personales;

VI. Implantar medidas de seguridad para el uso de los dispositivos electrónicos y físicos de salida, así como para evitar el retiro no autorizado de los mismos fuera de las instalaciones de la entidad o dependencia; y

VII. En el caso de requerirse disponibilidad crítica de datos, instalar y mantener el equipamiento de cómputo, eléctrico y de telecomunicaciones con la redundancia necesaria. Además, realizar respaldos que permitan garantizar la continuidad de la operación.

Seguridad en la red

Trigésimo segundo. En relación con los aspectos de seguridad al utilizar la red de comunicación donde se transmitan datos personales, es necesario establecer:

I. Procedimientos de control de acceso a la red que consideren perfiles de usuarios o grupos de usuarios para el acceso restringido a las funciones y programas de los Sistema de datos personales;

II. Mecanismos de auditoría o rastreabilidad de operaciones que mantenga una bitácora para conservar un registro detallado de las acciones llevadas a cabo en cada acceso, ya sea autorizado o no, a los Sistemas de datos personales.

Documento de seguridad

Trigésimo tercero. Las dependencias y entidades, a través del Comité y conjuntamente con el área de tecnología de la información, informática o su equivalente, expedirán un documento que contenga las medidas administrativas, físicas y técnicas de seguridad aplicables a los sistemas de datos personales, tomando en cuenta los presentes Lineamientos y las recomendaciones que en la materia emita el Instituto.

El documento de seguridad será de observancia obligatoria para todos los servidores públicos de las dependencias y entidades, así como para las personas externas que debido a la prestación de un servicio tengan acceso a los sistemas de datos personales y/o al sitio donde se ubican los mismos.

Requisitos del documento de seguridad

Trigésimo cuarto. El documento mencionado en el Lineamiento anterior deberá contener, como mínimo, los siguientes aspectos:

I. El nombre, cargo y adscripción de los Responsables, Encargados y Usuarios;

II. Estructura y descripción de los sistemas de datos personales;

III. Especificación detallada del tipo de datos personales contenidos en el sistema;

IV. Funciones y obligaciones de los servidores públicos autorizados para acceder al sitio seguro y para el tratamiento de datos personales;

V. Medidas, normas, procedimientos y criterios enfocados a garantizar el nivel de seguridad exigido en los presentes Lineamientos, las cuales deberán incluir lo siguiente:

a) Establecer procedimientos para generar, asignar, distribuir, modificar, almacenar y dar de baja usuarios y claves de acceso para la operación del Sistema de datos personales;
b) Actualización de información contenida en el Sistema de datos personales;
c) Procedimientos de creación de copias de respaldo y de recuperación de los datos;
d) Bitácoras de acciones llevadas a cabo en el Sistema de datos personales;
e) Procedimiento de notificación, gestión y respuesta ante incidentes; y
f) Procedimiento para la cancelación de un Sistema de datos personales.

El contenido del documento deberá actualizarse anualmente.

Registro de incidentes

Trigésimo quinto. El Encargado deberá llevar un registro de incidentes en el que se consignen los procedimientos realizados para la recuperación de los datos o para permitir una disponibilidad del proceso, indicando la persona que resolvió el incidente, la metodología aplicada, los datos recuperados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

Accesos controlados y bitácoras

Trigésimo sexto. En cada acceso a un Sistema de datos personales deberá guardarse como mínimo:

I. Datos completos del Responsable, Encargado o Usuario;
II. Modo de autenticación del Responsable, Encargado o Usuario;
III. Fecha y hora en que se realizó el acceso, o se intentó el mismo;
IV. Sistema de datos personales accedido;
V. Operaciones o acciones llevadas a cabo dentro del Sistema de datos personales; y
VI. Fecha y hora en que se realizó la salida del Sistema de datos personales.

Operaciones de acceso, actualización, respaldo y recuperación

Trigésimo séptimo. En las actividades relacionadas con la operación de los sistemas de datos personales tales como el acceso, actualización, respaldo y recuperación de información, las dependencias y entidades deberán llevar a cabo en forma adicional, las siguientes medidas:

I. Contar con manuales de procedimientos y funciones para el tratamiento de datos personales que deberán observar obligatoriamente los Responsables, Encargados o Usuarios de los sistemas de datos personales;

II. Llevar control y registros del Sistema de datos personales en bitácoras que contengan la operación cotidiana, respaldos, usuarios, incidentes y accesos, así como la transmisión de datos y sus destinatarios, de acuerdo con las políticas internas que establezca la dependencia o entidad;

III. Procedimientos de control de acceso a la red que incluyan perfiles de usuarios o grupos de usuarios para el acceso restringido a las funciones y programas de los sistemas de datos personales;

IV. Mecanismos de auditoría o rastreabilidad de operaciones;

V. Garantizar que el personal encargado del tratamiento de datos personales, sólo tenga acceso a las funciones autorizadas del Sistema de datos personales según su perfil de usuario;

VI. Aplicar procedimientos de respaldos de bases de datos y realizar pruebas periódicas de restauración;

VII. Llevar control de inventarios y clasificación de los medios magnéticos u ópticos de respaldo de los datos personales;

VIII. Utilizar un espacio externo seguro para guardar de manera sistemática los respaldos de las bases de datos de los sistemas de datos personales;

IX. Garantizar que durante la transmisión de datos personales y el transporte de los soportes de almacenamiento, los datos no sean accesados, reproducidos, alterados o suprimidos sin autorización;

X. Aplicar procedimientos para la destrucción de medios de almacenamiento y de respaldo obsoletos que contengan datos personales;

XI. En los casos en que la operación sea externa, convenir con el proveedor del servicio que la dependencia o entidad tenga la facultad de verificar que se respete la integridad, confiabilidad, confidencialidad y disponibilidad de los datos personales; revisar que el tratamiento se está realizando conforme a los contratos formalizados, así como que se cumplan los estándares de seguridad planteados en estos Lineamientos;

XII. Diseñar planes de contingencia que garanticen la continuidad de la operación y realizar pruebas de eficiencia de los mismos;

XIII. Llevar a cabo verificaciones a través de las áreas de tecnología de la información, informática o su equivalente respecto de medidas técnicas establecidas en los presentes Lineamientos y en su caso, remitirlos al Organo Interno de Control, y

XIV. Cualquier otra medida tendente a garantizar el cumplimiento de los principios de protección de datos personales señalados en el capítulo II de los presentes Lineamientos.

Estas medidas deberán ser integradas como anexos técnicos al documento de seguridad mencionado en el Lineamiento Trigésimo tercero.

Recomendaciones sobre estándares mínimos de seguridad

Trigésimo octavo. El Instituto emitirá anualmente las recomendaciones sobre los estándares mínimos de seguridad, aplicables a los sistemas de datos personales que se encuentren en poder de las dependencias y entidades de la

Administración Pública Federal y determinará en su caso, el nivel de protección que amerite la naturaleza de los datos personales.

Capítulo VI

Del Sistema "Persona"

Trigésimo noveno. Para dar cumplimiento a lo dispuesto por el artículo 23 de la Ley, el Instituto pondrá a disposición de las dependencias y entidades el Sistema "Persona".

Cuadragésimo. Los Responsables deberán registrar e informar al Instituto, dentro de los primeros diez días hábiles de enero y julio de cada año, lo siguiente:

a) Los sistemas de datos personales;

b) Cualquier modificación sustancial o cancelación de dichos sistemas, y

c) Cualquier transmisión de sistemas de datos personales de conformidad a lo dispuesto por los Lineamientos Vigésimo quinto y Vigésimo sexto de los presentes Lineamientos.

Datos del registro

Cuadragésimo primero. El registro de cada Sistema de datos personales deberá contener, los siguientes datos:

a) Nombre del sistema;

b) Unidad administrativa en la que se encuentra el sistema;

c) Nombre del responsable del sistema;

d) Cargo del Responsable;

e) Teléfono y correo electrónico del Responsable;

f) Finalidad del sistema, y

g) Normatividad aplicable al sistema.

El Instituto otorgará al Responsable un folio de identificación por cada Sistema de datos personales registrado.

Vínculo al Sistema "Persona"

Cuadragésimo segundo. Las dependencias y entidades deberán establecer un vínculo en sus sitios de Internet al Sistema "Persona", a efecto de dar cumplimiento a lo establecido en los artículos 48 y Sexto transitorio del Reglamento de la Ley.

Capítulo VII

Del Instituto

Supervisión de la Protección

Cuadragésimo tercero. Las dependencias y entidades deberán permitir a los servidores públicos del Instituto o a terceros previamente designados por éste, el acceso a los lugares en los que se encuentran y operan los sistemas de datos personales, así como poner a su disposición la documentación técnica y administrativa de los mismos, a fin de supervisar que se cumpla con la Ley, su Reglamento y los presentes Lineamientos.

Irregularidades

Cuadragésimo cuarto. En caso de que el Instituto determine que algún servidor público pudo haber incurrido en responsabilidades por el incumplimiento de los presentes Lineamientos, lo hará del conocimiento del Organo Interno de Control correspondiente, a efecto de que determine lo conducente, con base en el capítulo de Responsabilidades y Sanciones establecido en el Título IV de la Ley, así como en la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos.

Transitorios

Primero. Los presentes Lineamientos entrarán en vigor al día siguiente de su publicación en el Diario Oficial de la Federación.

Segundo. Los formatos y mecanismos mediante los cuales se recaben datos personales y se informe a los Titulares de los mismos sobre la finalidad del Sistema de datos personales, deberán ser elaborados o modificados en términos del Lineamiento Décimo Séptimo y deberán comenzar a utilizarse, a más tardar el día 31 de marzo de 2006.

En tanto, y a más tardar dentro de los 20 días hábiles siguientes a la entrada en vigor de los presentes Lineamientos las dependencias y entidades que recaben datos personales deberán entregar a los Titulares de los mismos un documento por separado en el que se informen los propósitos para los cuales éstos se recaban.

Tercero. El cumplimiento de las disposiciones contenidas en el capítulo V de los presentes Lineamientos deberá efectuarse a más tardar en diciembre de 2006, incluido el documento de seguridad a que se refiere el Lineamiento Trigésimo tercero.

Cuarto. La primera actualización del Sistema "Persona" por parte de las dependencias y entidades a que se refiere el Lineamiento Cuadragésimo, deberá llevarse a cabo dentro de los primeros diez días hábiles de marzo de 2006.

Quinto. Las primeras recomendaciones sobre las medidas de seguridad que se mencionan en el Lineamiento Trigésimo octavo, serán emitidas por el Instituto a más tardar en el mes de mayo de 2006.

Sexto. Se dejan sin efecto las disposiciones contenidas en los Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal para notificar al Instituto el listado de sus sistemas de datos personales, publicados el 20 de agosto de 2003 en el Diario Oficial de la Federación.

Así lo acordó por unanimidad el Pleno del Instituto Federal de Acceso a la Información Pública, en sesión celebrada el día veintisiete de julio de dos mil cinco, ante el Secretario de Acuerdos.- La Comisionada Presidenta, **María Marván Laborde**.- Rúbrica.- Los Comisionados: **Horacio Aguilar Alvarez de Alba**, **Alonso Gómez-Robledo Verduzco**, **Juan Pablo Guerrero Amparán**, **Alonso Lujambio Irazábal**.- Rúbricas.- El Secretario de Acuerdos, **Francisco Ciscomani Freaner**.- Rúbrica. **(R.- 218575)**