Instituto de Acceso
a la Información Pública

INSTITUTO DE ACCESO A LA INFORMACION PÚBLICA

REPUBLICA DE EL SALVADOR

LINEAMIENTOS GENERALES DE PROTECCION DE DATOS PERSONALES

PARA INSTITUCIONES DEL SECTOR PUBLICO

FEBRERO, 2016

El Instituto de Acceso a la Información Pública, con fundamento en lo dispuesto por el Decreto 534 del 30 de marzo del 2011 emitido por la Asamblea Legislativa, denominado "Ley de Acceso a la Información Pública;

CONSIDERANDO

I. 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;

II. Que la intimidad y privacidad es un derecho humano, siendo que el Estado tiene como límite el respeto a esa garantía fundamental de no intromisión en la vida privada, familiar, documentos, comunicaciones, con excepción de una orden judicial emitida por una autoridad competente, que justifique la intervención estatal en virtud de un proceso judicial o legal.

III. Observando que el artículo 6 constitucional establecen como límite a la manifestación de las ideas y a la libertad de imprenta respectivamente, el orden público, la moral, el honor, ni la vida privada.

IV. Que a su vez el acceso a la información pública está consagrado como derecho fundamental que el Estado está llamado a proteger. En este sentido, las instituciones públicas cumplen un papel fundamental en la promoción de la transparencia en su gestión, siendo los funcionarios públicos depositarios de la autoridad investida por la Nación.

V. Que los avances tecnológicos y el progreso de la sociedad de la información ofrecen a los individuos herramientas que contribuyen a mejorar su calidad de vida. Asimismo, coadyuvan con el Estado, a mejorar la actividad administrativa, el desarrollo económico, social y cultural, así como el cumplimiento de las obligaciones ciudadanas frente a éste. Por otra parte, las nuevas tecnologías facilitan ilimitadas posibilidades para transmitir 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;

VI. Que sin embargo, un tratamiento inadecuado de esas herramientas tecnológicas y de la información personal de los habitantes puede atentar contra la privacidad, seguridad y autodeterminación informativa de las personas al permitir que se generen formas de exclusión o condiciones de incertidumbre y riesgo,

VII. Que la Ley de Acceso a la Información Pública es obligatoria para los poderes públicos de la República de El salvador, 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;

VIII. Que el ejercicio de las atribuciones de las dependencias y entidades de la Administración Pública implica el tratamiento de 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 transferencia;

IX. Que es de gran relevancia que las personas tengan conocimiento de la información que de ellos obra en los archivos del Sector Público 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;

X. Que el Instituto 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, en equilibrio con los principios de Transparencia y Acceso a la Información Pública Gubernamental que se requieren para un desarrollo del Estado Democrático de Derecho;

POR TANTO

El Pleno del Instituto de Acceso a la Información Pública de la República de El Salvador, emite los siguientes,

LINEAMIENTOS DE PROTECCION DE DATOS PERSONALES PARA LAS INSTITUCIONES QUE CONFORMAN EL SECTOR PUBLICO

Capítulo I

Disposiciones generales

Artículo 1.- Objeto y ámbito de aplicación

Los presentes Lineamientos tienen por objeto establecer las políticas generales que deberán observar las dependencias y entidades de la Administración Pública para garantizar a la persona la facultad de decisión sobre el uso y destino de sus datos personales, con el propósito de:

a. Asegurar su adecuado tratamiento e impedir su uso para finalidades distintas de aquellas que motivaron se suministro.

b. Evitar la transferencia de datos personales ilícita y lesiva para la dignidad y derechos del afectado.

c. Instar a la Administración Pública a adoptar una cultura institucional y una concientización acerca de la importancia de poner en práctica los principios de acceso a la información pública y la transparencia, en equilibrio con el derecho de autodeterminación informativa y protección de datos de los administrados, con las limitaciones que establece la Ley.

Para tal efecto, los presentes lineamientos generales establecen 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 en el ejercicio de sus atribuciones.

Artículo 2.- Autodeterminación informativa

La autodeterminación informativa es el derecho fundamental, derivado del derecho al libre desarrollo de la personalidad y al respeto a su dignidad humana, que tiene por objeto de controlar el flujo de informaciones que conciernen a cada persona, evitando que se propicien acciones discriminatorias

Se reconoce el derecho de toda persona a la autodeterminación informativa, la cual abarca el conjunto de principios y garantías relativas al legítimo tratamiento de sus datos personales reconocidos en esta sección.

Artículo 3.- Definiciones

Para efectos de la aplicación de los presentes Lineamientos, además de las definiciones establecidas en el artículo 6 de la Ley de Acceso a la Información Pública, se entenderá por:

a. **Base de datos:** Cualquier archivo, fichero, registro u otro conjunto estructurado de datos personales públicos o privados, en el sitio o en la nube, que sean objeto de tratamiento, automatizado o manual, en el sitio o en la nube, bajo control o dirección de un responsable, cualquiera que sea la modalidad de su elaboración, organización o acceso.

b. **Consentimiento del titular de los datos personales:** Toda manifestación de voluntad, expresa, libre, inequívoca, informada y específica que se otorgue por escrito, para un fin determinado, mediante la cual el titular de los datos personales o su representante, consienta el tratamiento de sus datos personales.

c. **Datos de acceso público:** Aquellos archivos, registro u otro conjunto estructura de datos que pueden ser consultados por cualquier persona que no estén impedidos por una norma limitativa, o sin más exigencia que el pago de una contraprestación.

d. **Datos de acceso restringido:** Aquellos datos que, aun formando parte de registros de acceso al público, no son de acceso libre por ser de interés solo para su titular o para la Administración Pública.

e. **Datos en la nube:** Archivo, fichero, registro u otro conjunto estructurado de datos a los cuales se accesa haciendo uso de Internet

f. **Deber de confidencialidad:** obligación de los responsables de bases de datos, personal a su cargo y del personal del Instituto de Acceso a la Información Pública, de guardar la confidencialidad con ocasión del ejercicio de las facultades dadas por la ley, principalmente cuando se acceda a información sobre datos personales.

g. **Destinatario:** Cualquier persona física o jurídica o privada que recibe datos personales.

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

i. **Intermediario tecnológico o proveedor de servicios:** Persona física o jurídica, pública o privada que brinde servicios de infraestructura, plataforma, software u otros servicios, sin realizar tratamiento de datos personales.

j. **Instituto:** Instituto de Acceso a la Información Pública (IAIP)

k. **Persona física identificable:** Persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad anatómica, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionadas.

l. **Procedimiento de desasociación:** Acción y efecto de disociar los datos personales, de modo que la información que se obtenga no pueda asociarse o vincularse a persona determinada o determinable.

m. **Responsable:** El servidor público 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.

n. **Sistema de Registro:** 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.

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

p. **Transferencia:** 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.

q. **Transferente:** Dependencia o entidad que posee los datos personales objeto de la transferencia.

r. **Tratamiento:** Operaciones y procedimientos físicos o automatizados que permitan recabar, registrar, reproducir, conservar, organizar, modificar, transmitir y cancelar datos personales, entre otras acciones relacionadas.

s. **Tratamiento de datos automatizado:** Cualquier operación, conjunto de operaciones o procedimientos, aplicados a datos personales, efectuados mediante la utilización de hardware, software, redes, servicios, aplicaciones, en el sitio o en la nube, o cualquier otra tecnología de la información que permitan la recolección, el registro, la organización, la conservación, la modificación, la extracción, la consulta, la utilización, la comunicación por transferencia, difusión, distribución o cualquier otra forma que facilite el acceso a estos, el cotejo, o la interconexión, así como su bloqueo, supresión o destrucción, intercambio o digitalización de datos personales, entre otros.

Artículo 4.- Elementos de los datos personales

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

a. Que la misma sea concerniente a una persona física, identificada o identificable, y

b. Que la información se encuentre contenida en sus archivos.

Artículo 5.- Sistema de datos personales

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

Artículo 6.- Principios de la protección de datos personales

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

Artículo 7.- Licitud

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 de carácter personal serán recopilados con fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con dichos fines.

No se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando se establezcan las garantías oportunas para salvaguardar los derechos contemplados en esta ley.

Artículo 8.- Calidad de los datos

El tratamiento de datos personales deberá ser exacto, adecuado, actual, pertinente y no excesivo, respecto de las atribuciones legales de la dependencia o entidad que los posea. Asimismo, el responsable de la base de datos eliminará los datos que hayan dejado de ser pertinentes o necesarios, en razón de la finalidad para la cual fueron recibidos y registrados.

Para efectos de hacer valer el derecho al olvido en materia de protección de datos personales, en ningún caso serán conservados aquellos que puedan afectar, de cualquier modo, a su titular, una vez transcurridos diez años desde la fecha de ocurrencia de los hechos registrados, salvo disposición

normativa especial que disponga otra cosa. En caso de que sea necesaria su conservación, más allá del plazo estipulado, deberán ser desasociados de su titular

Artículo 9.- Exactitud

Los datos de carácter personal deberán ser exactos. La persona responsable de la base de datos tomará las medidas necesarias para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados.

Si los datos de carácter personal registrados resultan ser inexactos en todo o en parte, o incompletos, serán eliminados o sustituidos de oficio por la persona responsable de la base de datos, por los correspondientes datos rectificados, actualizados o complementados. Igualmente, serán eliminados si no media el consentimiento informado o está prohibida su recolección.

Artículo 10.- Acceso y corrección

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.

Artículo 11.- De Información

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.

Artículo 12.-Seguridad

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, reproducción, transferencia y acceso no autorizado.

Artículo 13.- Custodia y cuidado de la información

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

Artículo 14.- Consentimiento para la transferencia

Toda transferencia 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 Consentimiento

Artículo 15.- Del consentimiento informado

Cuando se soliciten datos de carácter personal será necesario informar de previo a las personas titulares o a sus representantes, de modo expreso, preciso e inequívoco:

a. De la existencia de una base de datos de carácter personal.

b. De los fines que se persiguen con la recolección de estos datos.

c. De los destinatarios de la información, así como de quiénes podrán consultarla.

d. Del carácter obligatorio o facultativo de sus respuestas a las preguntas que se le formulen durante la recolección de los datos.

e. Del tratamiento que se dará a los datos solicitados.

f. De las consecuencias de la negativa a suministrar los datos.

g. De la posibilidad de ejercer los derechos que le asisten.

h. De la identidad y dirección del responsable de la base de datos.

Quien recopile datos personales deberá obtener el consentimiento expreso de la persona titular de los datos o de su representante. Este consentimiento deberá constar por escrito, ya sea en un documento físico o electrónico, el cual podrá ser revocado de la misma forma, sin efecto retroactivo.

Artículo 16.- Excepciones al consentimiento informado

No será necesario el consentimiento expreso cuando:

a. Cuando fuere necesario por razones estadísticas, científicas o de interés general, siempre que no se identifique a la persona a quien se refieran.

b. Cuando se transmitan entre entes obligados, siempre y cuando los datos se destinen al ejercicio de sus facultades.

c. Cuando se trate de la investigación de delitos e infracciones administrativas, en cuyo caso se seguirán los procedimientos previstos en las leyes pertinentes.

d. Cuando exista orden judicial.

e. Cuando contraten o recurran a terceros para la prestación de un servicio que demande el tratamiento de datos personales. Los terceros no podrán utilizar los datos personales con propósitos distintos a aquellos para los cuales se les hubieren proporcionado y tendrán las responsabilidades legales que genere su actuación.

Artículo 17.- Formalidades del consentimiento informado

La obtención del consentimiento deberá ser:

a) Libre: no debe mediar error, mala fe, violencia física o psicológica o dolo, que puedan afectar la manifestación de voluntad del titular;

b) Específico: referido a una o varias finalidades determinadas y definidas que justifiquen el tratamiento;

c) Informado: que el titular tenga conocimiento previo al tratamiento, a qué serán sometidos sus datos personales y las consecuencias de otorgar su consentimiento. Asimismo, de saber quién es el responsable que interviene en el tratamiento de sus datos personales, y su lugar o medio de contacto;

d) Expreso: debe ser escrito e inequívoco, de forma tal que pueda demostrarse de manera indubitable su otorgamiento.

e) Individualizado: debe existir mínimo un otorgamiento del consentimiento por parte de cada titular de los datos personales.

Artículo 18.- Tratamiento exacto, adecuado, pertinente y no excesivo

A efecto de cumplir con el principio de calidad a que se refiere el artículo 8 de los presentes lineamientos, 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.

Artículo 19.- Corrección de oficio

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.

Artículo 20.- Conservación de los datos

Los datos personales que hayan sido objeto de tratamiento y no contengan valor histórico, científico, estadístico o contable, 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 Lineamientos relacionados con la Gestión Documental y Archivos emitidos por este Instituto, 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 transferencia.

Artículo 21.- Condiciones técnicas

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.

Artículo 22.- Derechos del titular

Se garantiza el derecho de toda persona al acceso de sus datos personales, rectificación o supresión de estos y a consentir la cesión de sus datos.

El Oficial de Información debe cumplir lo solicitado por el titular de los datos personales, tramitar de manera gratuita, y resolver en el sentido que corresponda en el plazo de diez días hábiles, contados a partir de la recepción de la solicitud. En caso de la rectificación, actualización, confidencialidad o

supresión de la información el plazo será de treinta días hábiles desde la presentación de la solicitud de información.

1.- Acceso a la información

La información deberá ser almacenada en forma tal que se garantice plenamente el derecho de acceso por la persona interesada.

El derecho de acceso a la información personal garantiza las siguientes facultades del interesado:

a. Obtener en intervalos razonables, según se dispone en la LAIP, sin demora y a título gratuito, la confirmación o no de la existencia de datos suyos en archivos o bases de datos. En caso de que sí existan datos suyos, estos deberán ser comunicados a la persona interesada en forma precisa y entendible.

b. Recibir la información relativa a su persona, así como la **finalidad** con que fueron recopilados y el uso que se le ha dado a sus datos personales. El informe deberá ser completo, claro y exento de codificaciones. Deberá estar acompañado de una explicación de los términos técnicos que se utilicen.

c. Ser informado por escrito de manera amplia, por medios físicos o electrónicos, sobre la totalidad del registro perteneciente al titular, aun cuando el requerimiento solo comprenda un aspecto de los datos personales. Este informe en ningún caso podrá revelar datos pertenecientes a terceros, aun cuando se vinculen con la persona interesada, excepto cuando con ellos se pretenda configurar un delito penal.

d. Tener conocimiento, en su caso, del sistema, programa, método o proceso utilizado en los tratamientos de sus datos personales.

2.- Derecho de rectificación

Se garantiza el derecho de obtener la rectificación de los datos personales y su actualización o la eliminación de estos cuando se hayan tratado con infracción a la ley, en particular a causa del carácter incompleto o inexacto de los datos, o hayan sido recopilados sin autorización del titular.

Todo titular puede solicitar y obtener del Oficial de Información, la rectificación, la actualización, la cancelación o la eliminación y el cumplimiento de la garantía de confidencialidad respecto de sus datos personales.

3.- Derecho de eliminación.

El titular podrá solicitar en cualquier momento al Oficial de Información, la eliminación total o parcial de los datos personales del titular, de manera definitiva.

Lo anterior salvo en los siguientes casos:

a. La seguridad del Estado;

b. Los datos deban ser mantenidos por disposición constitucional, legal o resolución de órgano judicial;

c. La seguridad ciudadana y el ejercicio de la autoridad pública;

d. La prevención, persecución, investigación, detención y represión de las infracciones penales, o de las infracciones de la deontología en las profesiones;

e. El funcionamiento de bases de datos que se utilicen con fines estadísticos, históricos o de investigación científica, cuando no exista riesgo de que las personas sean identificadas;

f. La adecuada prestación de servicios públicos;

g. La eficaz actividad ordinaria de la Administración, por parte de las autoridades oficiales;

h. Se trate de datos personales de acceso irrestricto, obtenidos de fuentes de acceso público general;

4.- Garantías efectivas

Toda persona interesada tiene derecho a un procedimiento sencillo y rápido ante el Instituto, con el fin de proteger sus datos personales reconocidos por la Ley de Acceso a la Información Pública y los presentes lineamientos. Lo anterior sin perjuicio de las garantías jurisdiccionales generales o específicas que la ley establezca para este mismo fin.

El ejercicio del derecho al cual se refiere este artículo, en el caso de datos de personas fallecidas, le corresponderá a sus presuntos sucesores o herederos.

Artículo 23.- Medios para recabar los datos

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 los artículos 15 y 16 de los presentes Lineamientos y 34 de la LAIP.

Artículo 24.- Disociación de datos

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 normativa vigente y demás disposiciones aplicables.

Artículo 25.- Tratamiento de datos por terceros

Cuando se contrate a terceros para que realicen el tratamiento de datos personales, deberá estipularse en el contrato respectivo las condiciones de utilización de los datos, la implementación de medidas de seguridad y custodia previstas en los presentes Lineamientos, así como la determinación de responsabilidades por su incumplimiento.

Artículo 26.- Procedimientos para el tratamiento.

El responsable establecerá y documentará procedimientos para la inclusión, conservación, modificación, bloqueo y supresión de los datos personales, en el sitio o en la nube, con base en los protocolos mínimos de actuación y las medidas de seguridad en el tratamiento de los datos personales. Además deberá el responsable de la base de datos velar por la aplicación del principio de calidad de la información.

Artículo 27.- Condiciones del tratamiento.

Corresponde al responsable o al encargado, la difusión, comercialización y distribución de dichos datos, según lo que determine el consentimiento informado otorgado por el titular, aún y cuando estos datos sean almacenados o alojados por un intermediario tecnológico.

Artículo 28.- Contratación o subcontratación de servicios.

Se podrá contratar o subcontratar los servicios del intermediario tecnológico o proveedor de servicios, siempre y cuando no implique tratamiento de datos personales. El responsable deberá verificar que dicho intermediario o proveedor cumpla con las medidas de seguridad mínimas que garanticen la integridad y seguridad de los datos personales.

Artículo 29.- Tratamiento de datos por parte del encargado.

El encargado solo podrá intervenir en el tratamiento de las bases de datos personales, según lo establecido en el contrato celebrado con el responsable y sus indicaciones.

Para tal efecto, el encargado tendrá las siguientes obligaciones en el tratamiento de las bases de datos personales:

a. Tratar únicamente los datos personales conforme a las instrucciones del responsable;

b. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable;

c. Implementar las medidas de seguridad y cumplir con los protocolos mínimos de actuación conforme a la Ley, los presentes lineamientos y las demás disposiciones aplicables;

d. Guardar confidencialidad respecto de los datos personales tratados;

e. Abstenerse de transferir o difundir los datos personales, salvo instrucciones expresas por parte del responsable.

f. Suprimir los datos personales objeto de tratamiento, una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales.

Capítulo IV
De la transferencia

Artículo 30.- Transferencia de los datos personales

Las dependencias y entidades sólo podrán transferir datos personales cuando:

a. Así lo prevea de manera expresa una disposición legal,

b. Medie el consentimiento expreso de los titulares,

El receptor de los datos transferidos podrá utilizarlos únicamente para los fines que motivaron la transferencia, salvo que se trate de datos personales accesibles al público en general o se transfieran datos personales a organizaciones internacionales en cumplimiento a Tratados vigentes.

Artículo 31.- Deber de informar al Instituto

Los Oficiales de Información deberán rendir informe a este Instituto, en los términos establecidos en los presentes Lineamientos, de las transferencias totales o parciales de sistemas de datos personales que realice el ente obligado.

Artículo 32.- Requisitos del Informe

El informe a que hace referencia el artículo anterior deberá contener al menos, lo siguiente:

a. Identificación del Sistema de datos personales, del transferente y del destinatario de los datos;

b. Finalidad de la transferencia; así como el tipo de datos que son objeto de la transferencia;

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

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

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

Capítulo V

De la Seguridad de los Sistemas de Datos Personales

Artículo 33.- Medidas de seguridad

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

a. Designar a los Responsables de acuerdo a la normativa aplicable a cada ente, los cuales deben tener conocimiento sobre la materia;

b. Proponer, 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;

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

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

Lo dispuesto en el literal "b" debe ser remitido al Instituto para dar cumplimiento al Art. 35 de la LAIP.

Artículo 34.- Acciones sobre seguridad

En cada dependencia o entidad, se designará una Comisión o Comité interdisciplinario que 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.

Artículo 35.- Reserva de la información

Los responsables podrán proponer la reserva de la documentación generada para la implementación, administración y seguimiento de las medidas de seguridad administrativa, física y técnica siempre y cuando coincida con las causales del Art. 19 de la LAIP.

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.

Artículo 36.- Resguardo de sistemas de datos personales físicos

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.

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

e. 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;

f. Contar con al menos dos lugares distintos, que cumplan con las condiciones de seguridad especificadas en los presentes lineamientos, destinados a almacenar medios de respaldo de sistemas de datos personales;

g. 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:

- Si es asignación, configurarlo con las medidas de seguridad necesarias, tanto a nivel operativo como de infraestructura, y
- Verificar y llevar un registro del contenido del equipo para facilitar los reportes del Usuario que lo recibe o lo entrega para su baja.

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

i. 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

j. 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.

Artículo 37.- Seguridad en la red

En relación con los aspectos de seguridad, al utilizar la red de comunicación donde se transfieran datos personales, será obligatorio por las entidades del Sector Público establecer:

a. 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;

b. 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 Sistema de datos personales.

Artículo 38.- Documento de seguridad

Las dependencias y entidades del Sector Público, 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.

Artículo 39.- Requisitos mínimos del documento de seguridad

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

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

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

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

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

e. Medidas, normas, procedimientos y criterios enfocados a garantizar el nivel de seguridad exigido en los presentes Lineamientos,

f. 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;

g. Actualización de información contenida en el Sistema de datos personales;

h. Procedimientos de creación de copias de respaldo y de recuperación de los datos;

i. Bitácoras de acciones llevadas a cabo en el Sistema de datos personales;

j. Procedimiento de notificación, gestión y respuesta ante incidentes; y

k. Procedimiento para la cancelación de un Sistema de datos personales.

El contenido del documento deberá actualizarse anualmente.

Artículo 40.- Registro de incidentes

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.

Artículo 41.- Accesos controlados y bitácoras

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

a. Datos completos del Responsable, Encargado o Usuario;
b. Modo de autenticación del Responsable, Encargado o Usuario;
c. Fecha y hora en que se realizó el acceso, o se intentó el mismo;
d. Sistema de datos personales accedido;
e. Operaciones o acciones llevadas a cabo dentro del Sistema de datos personales; y
f. Fecha y hora en que se realizó la salida del Sistema de datos personales.

Artículo 42.-Operaciones de acceso, actualización, respaldo y recuperación

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:

a. 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;

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

c. 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;

d. Mecanismos de auditoría o rastreabilidad de operaciones;

f. 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;

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

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

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

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

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

k. 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;

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

m. 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 Órgano Interno de Control, y

o. 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 Artículo 38 de los presentes Lineamientos.

Capítulo VI

Registro del Sistema de datos personales

Artículo 43.- 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 transferencia de sistemas de datos personales de conformidad a lo dispuesto por los Lineamientos Vigésimo quinto y Vigésimo sexto de los presentes Lineamientos.

Artículo 44.-Datos del registro

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.

Capítulo VII

Del Instituto

Artículo 45.- Atribuciones

Son atribuciones del Instituto, además de las otras que le impongan la Ley u otras normas, las siguientes en materia de protección de datos personales:

a. Velar por el cumplimiento de la normativa en materia de protección de datos.

b. Llevar un registro de las bases de datos reguladas por esta ley.

c. Requerir, de quienes administren bases de datos, la información necesaria para el ejercicio de su cargo.

d. Acceder a las bases de datos reguladas por los presentes lineamientos, a efectos de hacer cumplir efectivamente las normas sobre protección de datos personales. Esta atribución se aplicará para los casos concretos presentados ante el Instituto, excepcionalmente, cuando se tenga evidencia de un mal manejo generalizado de la base de datos o sistema de información.

e. Resolver sobre los reclamos por infracción a las normas sobre protección de los datos personales.

f. Ordenar, de oficio o a petición de parte, la supresión, rectificación, adición o restricción en la circulación de la información contenida en los archivos y las bases de datos, cuando estas contravengan las normas sobre protección de los datos personales.

g. Promover y contribuir en la redacción de normativa tendiente a implementar las normas sobre protección de los datos personales.

h. Dictar las directrices necesarias, las cuales deberán ser publicadas en el diario oficial, a efectos de que las instituciones públicas implementen los procedimientos adecuados respecto del manejo de los datos personales, respetando los diversos grados de autonomía administrativa e independencia funcional.

i. Fomentar entre los habitantes el conocimiento de los derechos concernientes al acopio, el almacenamiento, la transferencia y el uso de sus datos personales.

En el ejercicio de sus atribuciones, el Instituto deberá emplear procedimientos automatizados, de acuerdo con las mejores herramientas tecnológicas a su alcance.

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.

Capítulo VII

Disposiciones transitorias

Artículo 46.- 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 en términos de los presentes Lineamientos y deberán comenzar a utilizarse, a más tardar en un plazo de un año a partir de la vigencia de los presentes lineamientos.

Artículo 47.- En tanto, y a más tardar dentro de un mes siguiente a la entrada en vigor de los presentes Lineamientos las dependencias y entidades que recaben datos personales deberán informar a los Titulares de los mismos un documento por separado en el que se detalle los propósitos para los cuales éstos se recaban.

Artículo 48.- El cumplimiento de las disposiciones contenidas en el los presentes Lineamientos deberá efectuarse a más tardar en un plazo de seis meses posterior a su entrada en vigor, incluido el documento de seguridad y registro de bases de datos al cual se refiere el Lineamiento Trigésimo tercero.

Artículo 49.- El Instituto deberá efectuar las siguientes acciones:

a. Elaborar e iniciar un plan de capacitación sobre datos personales dirigida al Sector Público con el fin de implementar los presentes lineamientos y el manual de protección de datos, en un plazo máximo de un mes a partir de la publicación de este último.

b. Elaborar las recomendaciones sobre las medidas de seguridad que se mencionan en los presentes Lineamientos, a más tardar en un plazo de un mes a partir de su entrada en vigor.

Capítulo VIII

Disposiciones finales

Artículo 50.- Los presentes Lineamientos entrarán en vigor un año después de su publicación en el Diario Oficial.

Artículo 51.- Así lo acordó por unanimidad el Instituto de Acceso a la Información Pública, en sesión celebrada el veintidós de febrero de dos mil dieciséis.-

Los Comisionados Propietarios, **Carlos Adolfo Ortega Umaña, Jaime Mauricio Campos Pérez, Max Fernando Mirón Alfaro, María Herminia Funes de Segovia, Mauricio Antonio Vásquez López.**- Rúbrica.-