LINEAMIENTOS GENERALES Y RECOMENDACIONES PARA LA PROTECCIÓN DE DATOS PERSONALES.

C O N S I D E R A N D O

I. Que en atención a las garantías individuales que establece la Constitución Política de los Estados Unidos Mexicanos las que han sido reiteradas por la Constitución Local del Estado, se reconoce el respeto a la dignidad de la persona, el cual es un valor central de los estados democráticos que tienen como finalidad la búsqueda de la justicia, la libertad, la igualdad, la seguridad y la solidaridad, y que es a partir de la conciencia y de la afirmación de dicha dignidad que existen y se legitiman todos los derechos;

II. Considerando que fue voluntad del legislador plasmar en la Constitución General de la República el derecho a la vida privada, 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 o a la vida privada tiene dos factores fundamentales que son: una tutela a 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;

III. Observando que los artículos 6 y 7 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. De igual forma el artículo 6 constitucional establece el derecho a la información, mismo que será garantizado por el Estado, y de conformidad con lo dispuesto por el artículo 6 constitucional fracciones II y III, se expiden los presentes lineamientos generales y recomendaciones para la protección de datos personales;

IV. 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;

V. 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;

VI. Reconociendo que como consecuencia de lo anterior, 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;

VII. Tomando en cuenta que la Ley que Garantiza la Transparencia y el Derecho a la Información Pública para el Estado de Chiapas, es obligatoria únicamente para los Sujetos Obligados a que hace referencia el artículo 2 de dicho ordenamiento legal y tiene como uno de sus principios rectores el de garantizar la protección de los datos personales en posesión de éstos, así como el acceso y la corrección de los mismos.

VIII. Reconociendo que en el ejercicio de sus funciones y en cumplimiento de sus atribuciones, los Organismos Públicos tienen la necesidad de 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, atendiendo los principios de protección de datos personales de licitud, calidad, de informar 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;

IX. Considerando que los Sujetos Obligados deben 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 señalados en la Ley que Garantiza la Transparencia y el Derecho a la Información Pública para el Estado de Chiapas, por lo que ante una solicitud de acceso a información gubernamental, en la que se requieran datos personales, los Organismos Públicos, 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 35 segundo párrafo y 37 de la Ley; y

X. El Instituto de Acceso a la Información Pública de la Administración Pública Estatal es el órgano garante de la protección de los datos personales 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 II del Título Tercero de la Ley que Garantiza la Transparencia y el Derecho a la Información Pública para el Estado de Chiapas, requieren de un desarrollo para su adecuada observancia; en consecuencia, el Instituto tiene la facultad de expedir lineamientos y recomendaciones para asegurar y propiciar el cumplimiento de la ley, como consecuencia, con base en las facultades que le otorgan la ley al Pleno del Instituto, ha tenido a bien expedir los siguientes:

LINEAMIENTOS GENERALES Y RECOMENDACIONES PARA LA PROTECCIÓN DE DATOS PERSONALES.

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1. Los presentes lineamientos tienen por objeto establecer las políticas generales y procedimientos que deberán observar los sujetos obligados señalados en el numeral 2 de la Ley que Garantiza la Transparencia y el Derecho a la Información Pública para el Estado de Chiapas, para efectos de 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 manejo ilícito y lesivo 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 personales que se encuentren en posesión de los sujetos obligados, en el ejercicio de sus atribuciones.

Artículo 2. A efecto de determinar si la información que posee un Organismo Público constituye un dato personal, deberán agotarse las siguientes condiciones:

I. Que la misma sea concerniente a una persona física, identificada o identificable, en los términos de la disposición vigésima tercera de los lineamientos generales y recomendaciones para la clasificación y desclasificación de la información.
II. Que la información se encuentre contenida en sus archivos.

Artículo 3. Para efectos de la aplicación de los presentes Lineamientos Generales y Recomendaciones, además de las definiciones establecidas en el artículo 3 de la Ley que Garantiza la Transparencia y el Derecho a la Información Pública para el Estado de Chiapas y las referidas en los Lineamientos expedidos por este Instituto, 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. **Responsable:** El servidor público titular de la unidad administrativa designado por el titular del sujeto obligado, que decide sobre el tratamiento físico o automatizado de datos personales, así como el contenido y finalidad de los datos personales.
IV. **Titular de los datos:** Persona física a quien se refieren los datos personales que sean objeto de tratamiento.
V. **Transmisión:** Toda entrega total o parcial de datos, banco de datos, o sistemas de datos personales realizada por los sujetos obligados 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.
VI. **Transmisor:** Dependencia o entidad que posee los datos personales objeto de la transmisión.
VII. **Tratamiento:** Operaciones y procedimientos físicos o automatizados que permitan recabar, registrar, reproducir, conservar, organizar, modificar, transmitir y cancelar datos personales.
VIII. **Usuario:** Servidor público facultado por un instrumento jurídico, normativo 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.
IX. **Sistema de Datos Personales:** Conjunto ordenado de datos personales que estén en posesión del Sujeto Obligado, con

independencia de su forma de acceso, creación, almacenamiento u organización.

Artículo 4. En atención a lo que dispone el artículo 42 de la ley, con relación a sistematizar en archivos los datos personales que obren en su poder, los sujetos obligados deberán implementar un sistema de datos personales acorde a sus necesidades de organización, así también, considerando su capacidad presupuestaria y técnica para tales efectos.

En este sentido 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 5. En el tratamiento de datos personales, los Sujetos Obligados deberán observar los principios de licitud, calidad, acceso y corrección, de información, seguridad, custodia y consentimiento para su manejo y transmisión.

Artículo 6. La posesión de sistemas de datos personales deberá obedecer exclusivamente a las atribuciones legales o reglamentarias de cada Sujeto Obligado 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.

Artículo 7. El tratamiento de datos personales deberá ser exacto, adecuado, pertinente y no excesivo, respecto de las atribuciones legales y normativos del Organismo Público que los posea.

Artículo 8. Los sistemas de datos personales deberán implementarse y almacenarse de forma tal que permitan el ejercicio de los derechos de acceso y corrección previstos por la Ley y los Lineamientos emitidos por el Instituto.

Artículo 9. 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 10. 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.

Artículo 11. Los datos personales serán debidamente custodiados y los Responsables, Encargados y Usuarios deberán garantizar el manejo cuidadoso en su tratamiento.

Artículo 12. Toda solicitud, entrega o 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 por la Ley y lo establecido en el artículo 22 de los presentes Lineamientos Generales y Recomendaciones.

CAPÍTULO III
DEL TRATAMIENTO

Artículo 13. A efecto de cumplir con el principio de calidad a que se refiere el artículo 7, 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 protección, conservación y de seguridad aplicables;
c) **Pertinente:** Cuando es realizado por el personal autorizado para el cumplimiento de las atribuciones de los sujetos obligados que los resguarde o los haya 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 14. En caso de que se detecten que hay datos personales inexactos, los sujetos obligados, a través del Responsable del sistema de datos personales, 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 15. El periodo de conservación de los datos personales, no deberá exceder del necesario para alcanzar la finalidad con que se han registrado, teniendo en cuenta los siguientes aspectos:

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 el Organismo Público, y
d) El señalado en los casos de transmisión.

Artículo 16. Los datos personales sólo podrán ser tratados en sistemas de datos personales que reúnan las condiciones técnicas de integridad y de seguridad para el debido resguardo de la información.

Artículo 17. En el momento en que se recaben datos personales, el Sujeto Obligado, 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. (Físico o automatizado según sea el caso).

Artículo 18. Sin perjuicio de que los sujetos obligados, elaboren sus propios formatos para informar al Titular de los datos lo establecido por el artículo 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),y podrán ser transmitidos a (indicar 4), con el objeto 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 al artículo 43 de la Ley y 17 de los presentes Lineamientos de Protección de Datos Personales publicados en la página web del Instituto (incluir fecha8).

1. *Indicar el nombre del sistema de datos personales.*
2. *Indicar el fundamento legal que faculta a la dependencia, entidad u organismo público 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 información del Sujeto Obligado que posea el sistema de datos personales.*
8. *Anotar la fecha de publicación de los presentes lineamientos en la página web del Instituto.*

Artículo 19. Los Sujetos Obligados 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 artículo 17 de los presentes Lineamientos.

Artículo 20. 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 las disposiciones aplicables en la materia.

Artículo 21. 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 Generales y Recomendaciones, en la normatividad aplicable a los

Sujetos Obligados contratantes, así como la imposición de sanciones convencionales por su incumplimiento.

CAPÍTULO IV
DEL ACCESO Y CORRECCIÓN DE DATOS PERSONALES

Artículo 22. Para efectos de la Ley y los presentes Lineamientos Generales y Recomendaciones, los datos personales se consideraran información confidencial, los cuales solo podrán darse a conocer o transmitir con el consentimiento expreso del titular de los datos.

Artículo 23. Es obligación de los Sujetos Obligados dar trámite a las solicitudes de acceso o corrección de Datos Personales, a través de la Unidad de Información Pública correspondiente.

Artículo 24. Las solicitudes de acceso o corrección de Datos Personales, deberán cumplir con los requisitos establecidos en el artículo 16 de la Ley.

Artículo 25. El procedimiento de trámite de solicitud de acceso o corrección de Datos Personales, será el mismo establecido en el artículo 17 de la Ley.

Artículo 26. Toda solicitud de información de acceso o corrección de Datos Personales, deberá ser resuelta en los mismos plazos que se establecen en el artículo 20 de la Ley.

CAPÍTULO V
DE LA TRANSMISIÓN

Artículo 27. Los sujetos obligados, podrán proporcionar o transmitir datos personales sin el consentimiento del Titular de los datos, en los casos previstos en el artículo 45 de la Ley. Asimismo, deberán otorgar acceso a aquellos datos que no se consideran como confidenciales por ubicarse en los supuestos establecidos por el artículo 35 último párrafo.

Artículo 28. Para los efectos del artículo 35 de la Ley y en los casos no previstos por el artículo 45 de la Ley, los Sujetos Obligados sólo podrán transmitir datos personales cuando:

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

Artículo 29. Para la entrega o 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.

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

CAPÍTULO VI
DE LA SEGURIDAD DE LOS SISTEMAS DE DATOS PERSONALES

Artículo 30. Para proveer seguridad a los sistemas de datos personales, los titulares de los Sujetos Obligados, 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 de Información la difusión de la normatividad entre el personal involucrado en el manejo de los sistemas de datos personales, y
- **IV.** Proponer al Comité de Información la elaboración de un plan de capacitación en materia de protección y seguridad de datos personales dirigida a los Responsables, Encargados y Usuarios.

Artículo 31. El Comité de Información 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. Para ello, el responsable de las unidad de información pública deberá proponer los mecanismos y procedimientos para el cumplimiento de estas actividades.

Artículo 32. 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.

Artículo 33. El Responsable del sistema de datos personales 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 o normativo, a Usuarios, y llevar una relación actualizada de las personas que tengan acceso a los sistemas de datos personales que se encuentran en soporte físico, e
c) Informar al Comité de Información de los Usuarios.

Artículo 34. A los Sujetos Obligados que implementen sistemas de datos persónales automatizados, se recomiendan las siguientes consideraciones:

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 Generales y Recomendaciones, 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 del Organismo Público; 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.

Artículo 35. Aquellos sujetos obligados que procesen, almacenen o transmitan datos personales a través de una red de comunicación se recomienda establecer aspectos de seguridad, tales como:

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 sistemas de datos personales;
II. Mecanismos de auditoria 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.

Artículo 36. Los Sujetos Obligados, a través de su Comité de Información y conjuntamente con el responsable de la Unidad de Información Pública, y con el área técnica (informática o sistemas) 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 Generales y Recomendaciones que en la materia emita el Instituto.

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

Artículo 37. El documento mencionado en el artículo 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 a los documentos 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 Generales y Recomendaciones, 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.

TRANSITORIOS

Primero. Los presentes Lineamientos Generales y Recomendaciones entrarán en vigor al día siguiente de su publicación en la página web del Instituto.

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 artículo 17 de los presentes Lineamientos Generales y Recomendaciones.

Tercero. Las solicitudes de acceso o corrección de datos personales iniciarán a partir del 1º de Septiembre de 2007.

Cuarto. Los sujetos obligados deberán informar al Instituto dentro de los seis meses posteriores a la entrada en vigor de los presentes Lineamientos Generales y Recomendaciones, la puesta en operación del Sistema de Datos Personales respectivo, en los términos que se establecen en el artículo 42 de la Ley, sin detrimento que durante este lapso y en todo momento, se instrumenten las medidas y procedimientos para la protección de los datos personales, dando cumplimiento a las disposiciones legales y normativas en la materia.

Así lo acordó por unanimidad el Pleno del Instituto de Acceso a la Información Pública de la Administración Pública Estatal, en sesión ordinaria celebrada el día ocho de agosto de dos mil siete, ante el Secretario de Acuerdos del Pleno.- El Consejero General, Lic. Gildardo Arturo Domínguez Ruíz.- Rúbrica.- Consejera, Dra. María Elena Tovar González.- Rúbrica.- Consejero, Lic. Hermann Hoppenstedt Pariente.- Rúbrica.- El Secretario de Acuerdos del Pleno. Lic. Gerardo Aguilar Yáñez.- Rúbrica.