Considerando:

Que la protección de datos personales, asociada a la privacidad y la intimidad, se ha erigido en un derecho fundamental en sí mismo, en particular en el contexto de la sociedad de la información y el conocimiento;

Que, en el Estado de Oaxaca, la Ley de Protección de Datos Personales, que garantiza ese derecho fundamental, entró en vigor el pasado veinticuatro de agosto de dos mil ocho y establece al Instituto Estatal de Acceso a la Información la obligación de emitir, en un plazo determinado, los Lineamientos correlativos para el manejo, mantenimiento, seguridad y protección de los datos personales;

Con fundamento en los artículos 47 de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Oaxaca, y los numerales 41, fracciones IV y V, y 26, fracción III, y el Transitorio Segundo de la Ley de Protección de Datos Personales del Estado de Oaxaca, el Pleno del Instituto Estatal de Acceso a la Información Pública, expide los siguientes:

LINEAMIENTOS DE PROTECCION DE DATOS PERSONALES

TÍTULO PRIMERO

Capítulo I

Disposiciones generales y principios

Objeto y ámbito de aplicación

Primero. Los presentes Lineamientos tienen por objeto establecer las políticas generales que deberán observar las dependencias y entidades de las Administraciones Públicas Estatal, Municipal y demás sujetos obligados señalados en el artículo 5 de la Ley de Protección de Datos Personales para garantizar a la persona, protección, seguridad y adecuado tratamiento de sus datos personales, con el fin de impedir su transmisión ilícita y lesiva.

Estos lineamientos establecen las condiciones y requisitos mínimos obligatorios para la debida custodia y manejo de los sistemas de datos personales en posesión de los sujetos obligados.

Elementos de los datos personales

Segundo. A efecto de determinar si la información que posee un sujeto obligado constituye un dato personal, deberán cumplirse las siguientes condiciones:

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

2) Que la información se encuentre en sus archivos y sea la señalada en el artículo 6 fracc. I de la Ley de la materia.

Definiciones

Tercero. Para efectos de la aplicación de los presentes Lineamientos, además de las definiciones establecidas en los artículos 3 de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Oaxaca, 2 de su Reglamento y 6 de la Ley de Protección de Datos Personales, 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 facultados 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 Multimedia de Registro de Datos Personales. Aplicación informática desarrollada por el Instituto, para mantener actualizado el listado de los sistemas de datos personales que posean los sujetos obligados con el fin de registrar e informar sobre la creación, modificación, cancelación y transmisión de los mismos.

IV. Responsable: El titular de la unidad administrativa encargada de decidir sobre el tratamiento de los datos personales, así como el contenido y finalidad de estos sistemas.

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 por cualquier medio realizada por las dependencias y entidades a personas distintas al Titular de los datos, a través del uso de medios físicos o electrónicos tales como la interconexión de computadoras, de bases de datos, acceso a redes de telecomunicación o aplicación 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 sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, evaluación, bloqueo, destrucción, administración y, en general el procesamiento de datos personales; así como su cesión a terceros.

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.

X.- Reglamento: El Reglamento Interior del Recurso de Revisión y demás procedimientos del Instituto Estatal de Acceso a la Información Pública.

XI.- Ley de Archivos: Ley de Archivos del Estado de Oaxaca.

Sistema de datos personales

Cuarto. Un Sistema de datos personales constituye el conjunto ordenado de datos personales en posesión de los sujetos obligados, contenidos en archivos, registros, ficheros, bases o sistemas de datos, cualquiera que fuere la modalidad de su creación, almacenamiento, organización o acceso.

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

Quinto. En el tratamiento de datos personales, los sujetos obligados deberán observar los principios de licitud, calidad de la información, seguridad, confidencialidad, consentimiento, disponibilidad e integridad.

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 fundada y motivada.

Calidad de la información

Séptimo. Los datos personales recabados y su tratamiento deben ser veraces, adecuados, pertinentes y no excesivos, en relación al ámbito y finalidad para los que se hubieren obtenido.

Seguridad

Octavo. Los sujetos obligados deberán elaborar documentos de seguridad que establezcan las medidas físicas, técnicas y administrativas necesarias para garantizar la integridad, confiabilidad, confidencialidad y disponibilidad de los datos personales para evitar su alteración, pérdida, transmisión y acceso no autorizado.

Confidencialidad

Noveno. Consiste en garantizar que exclusivamente el Titular o la persona autorizada por éste, pueda acceder a sus datos personales a menos que medie disposición legal. El responsable o usuarios del sistema de datos personales tienen el deber de secrecía en el tratamiento de aquéllos. Esta obligación subsistirá aún finalizada la relación entre el ente público con el titular de los datos personales o concluida la relación laboral entre el ente público y el responsable del sistema de datos personales o los usuarios.
El responsable y usuarios del sistema de datos personales podrán ser relevados del deber de confidencialidad por resolución judicial o cuando medien razones fundadas relativas a la seguridad o salud públicas, estatales o nacionales.

Consentimiento

Décimo. Toda transmisión de datos personales deberá contar con el consentimiento de su Titular. Dicho consentimiento deberá otorgarse en forma libre, expresa e informada, salvo lo dispuesto en el Lineamiento Vigésimo primero.

Disponibilidad e Integridad

Décimo Primero. Los datos deben ser almacenados de modo que permitan el ejercicio de los derechos de acceso, rectificación, cancelación y oposición durante el tiempo que permanezcan en posesión de los sujetos obligados y deberán ser destruidos cuando hayan dejado de ser necesarios y pertinentes a los fines para los que hubiesen sido recabados.

Únicamente podrán ser conservados de manera íntegra, permanente y sujetos a tratamiento, cuando se trate para fines científicos, estadísticos e históricos.

TÍTULO SEGUNDO
Capítulo III
Del Tratamiento

Tratamiento exacto, adecuado, pertinente y no excesivo

Decimo segundo. A efecto de cumplir con el principio de calidad de la información 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 alteren la veracidad de la información ni traigan 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 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

Décimo tercero. Cuando los Responsables, Encargados o Usuarios detecten la existencia de datos personales inexactos, deberán de oficio, actualizarlos en el momento en que tengan conocimiento de la inexactitud, siempre que posean los documentos justificatorios de la actualización.

Conservación de los datos

Décimo cuarto. Los datos personales que hayan sido objeto de tratamiento y no contengan valores históricos, científicos, estadísticos, deberán ser dados de baja por los sujetos obligados, o bien, los que contengan dichos valores serán objeto de transferencias secundarias, de acuerdo con lo dispuesto por la Ley de Archivos.

Condiciones técnicas

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

Información al Titular de los datos

Décimo sexto. En el momento en que se recaben datos personales, los sujetos obligados deberán hacer del conocimiento del Titular de los datos tanto en los formatos físicos como en los electrónicos utilizados para ese fin, lo siguiente:

a. El nombre del sistema de datos personales al que se incorporaran sus datos personales, la finalidad y destinatarios del mismo.
b. El cargo, dirección, teléfono y correo electrónico oficiales de la Unidad Administrativa responsable del sistema de datos personales.
c. Del carácter obligatorio o facultativo de la entrega de los datos personales.
d. De las consecuencias de la negativa a suministrarlos.

e. De la posibilidad que estos datos sean transmitidos, en cuyo caso deberá constar el consentimiento expreso de la persona así como la mención en los casos que esta transmisión sea por disposición legal.
f. De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación u oposición agregando la ubicación de la Unidad de Enlace correspondiente;

Modelo de leyenda para informar al Titular de los datos

Decimo séptimo. Sin perjuicio de que los sujetos obligados 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, incorporados y tratados en el Sistema de datos personales[1], con fundamento en[2] y cuya finalidad es [3], el cual fue registrado en el Listado de sistemas de datos personales ante el Instituto Estatal de Acceso a la Información Pública (www.ieaip.org.mx), y podrán ser transmitidos a[4], con la finalidad de[5], además de otras transmisiones previstas en la Ley. La Unidad Administrativa responsable del Sistema de datos personales es[6], y la dirección donde el interesado podrá ejercer los derechos de acceso, rectificación, cancelación y oposición ante la misma es[7]. Lo anterior se informa en cumplimiento del Décimo sexto de los Lineamientos de Protección de Datos Personales, publicados en la página electrónica www.ieaip.org.mx[8].

Otros medios para recabar los datos

Décimo octavo. Los sujetos obligados que recaben datos personales a través de otros medios o sistemas, deberán informar al Titular de éstos, la finalidad de dicho acto así como el tratamiento al cual serán sometidos, cumpliendo con lo establecido en el Decimo sexto de los presentes Lineamientos.

Disociación de datos

Décimo noveno. La disociación es el tratamiento de los datos personales de modo que los datos resultantes no puedan relacionarse de ninguna forma o medio con persona identificada o identificable.

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 (LIEG), así como las demás disposiciones aplicables.

---

[1] Indicar el nombre de datos personales
[2] Indicar el fundamento legal que faculta a los sujetos obligados para recabar los datos personales en el sistema
[3] Describir la finalidad del sistema de datos personales
[4] Indicar las personas u organismos a las que podrán transmitirse los datos personales en el sistema
[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 del sujeto obligado que posee el sistema
[8] Anotar la fecha de publicación de entrada en vigor

Tratamiento de datos por terceros

Vigésimo. Los contratos de servicios en que consten las facultades de terceros para acceder y tratar sistemas de datos personales deberán prever la obligación de garantizar la seguridad y confidencialidad de los sistemas; así como la prohibición de utilizarlos con propósitos distintos para los cuales se llevó a cabo la contratación, así como las penas convencionales por su incumplimiento. Lo anterior, sin perjuicio de las responsabilidades previstas en otras disposiciones aplicables.

Capítulo IV
De la transmisión

Transmisión sin consentimiento del Titular de los datos

Vigésimo primero. Los sujetos obligados podrán transmitir datos personales sin el consentimiento del Titular, en los casos previstos por el artículo 7 de la Ley de Protección de datos Personales.

Transmisión con el consentimiento del Titular de los datos

Vigésimo segundo. Los sujetos obligados 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.

Vigésimo tercero. En relación con lo dispuesto por el numeral Décimo de estos lineamientos, 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, los sujetos obligados deberán cumplir con las disposiciones aplicables en materia de certificados digitales y/o firmas electrónicas.

El servidor público encargado de transmitir datos personales deberá recabar en forma previa a cada transmisión, el consentimiento del Titular. Advirtiéndole las implicaciones de otorgar su consentimiento.

Informes sobre la transmisión

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

Requisitos del Informe

Vigésimo quinto. 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 sean objeto de aquélla;

III. Las medidas de protección, seguridad y conservación adoptadas por el transmisor y destinatario;

IV. Tiempo por el que conservará el destinatario los datos que le hayan sido transmitidos, el cual podrá ser prorrogado por un plazo igual mediante aviso al Instituto dentro de los quince días hábiles previos al vencimiento; 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 misma.

Capítulo V
De la Seguridad de los Sistemas de Datos Personales

Medidas de seguridad

Vigésimo sexto. 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, así como las medidas de seguridad física, técnica y administrativa 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. Solicitar al Instituto Estatal de Acceso a la Información Pública los programas de capacitación necesarios en materia de seguridad de datos personales dirigida a los Responsables, Encargados y Usuarios.

Acciones sobre seguridad

Vigésimo séptimo. En cada sujeto obligado, el Comité de información coordinará y supervisará las acciones de difusión, 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.

Reserva de la información

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

Resguardo de sistemas de datos personales físicos

Vigésimo noveno. 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, tratamiento o acceso no autorizado;

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

c) Comunicar al Comité de Información así como al Instituto Estatal de Acceso a la Información los nombres de los Encargados y Usuarios con la periodicidad señalada en el numeral cuadragésimo quinto de estos lineamientos.

Sitio seguro para sistemas de datos personales automatizados

Trigésimo. Los sujetos obligados deberán:

I. De acuerdo con su disponibilidad presupuestal, asignar espacios seguros y adecuados para la operación de los sistemas de datos personales físicos y electrónicos**,** contando con al menos dos lugares distintos, que cumplan con las condiciones de seguridad especificadas en estos Lineamientos, destinados a almacenar medios de respaldo de estos sistemas;

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

III. Establecer procedimientos de control, supervisión, 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.

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

V. 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

VI. 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.

Las medidas anteriores y las que tengan como propósito superar y mejorar la seguridad de los sistemas de datos personales, deberán ser aprobadas por el Instituto Estatal de Acceso a la Información Pública a través del Registro Estatal de Protección de Datos Personales.

Seguridad en la red

Trigésimo primero. 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 sistemas 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.

El Instituto Estatal de Acceso a la Información Pública emitirá opinión sobre los proyectos de los procedimientos de control y mecanismos de auditoría autorizados.

Documento de seguridad

Trigésimo segundo. Los sujetos obligados, a través del Comité de Información 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 los sujetos obligados, 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 tercero. 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 periódica 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 y baja de un sistema de datos personales.

El contenido del documento deberá actualizarse anualmente.

Registro de incidentes

Trigésimo cuarto. 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 quinto. 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 sexto. En las actividades relacionadas con la operación de los sistemas de datos personales tales como el acceso, actualización, respaldo y recuperación de información, los sujetos obligados 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 establezcan 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 el perfil del 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 el sujeto obligado 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 Órgano Interno de Control; y

XIV. Cualquier otra medida tendiente 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 segundo.

Recomendaciones sobre estándares mínimos de seguridad

Trigésimo séptimo. 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 los sujetos obligados y determinará el nivel de protección que amerite la naturaleza de los datos personales.

Trigésimo octavo. El ente público responsable de la tutela y tratamiento de los sistemas de datos personales, adoptará las medidas de seguridad conforme a lo siguiente:

Tipos de seguridad

Física.- Se refiere a toda medida orientada a la protección de instalaciones, equipos, soportes o sistemas de datos para la prevención de riesgos por caso fortuito o causa de fuerza mayor;

Lógica.- Se refiere a las medidas de protección que permiten la identificación y autenticación de las personas o usuarios autorizados para el tratamiento de los datos personales de acuerdo con su función;

De desarrollo y aplicaciones.- Corresponde a las autorizaciones con las que deberá contar la creación o tratamiento de sistemas de datos personales, según su importancia, para garantizar el adecuado desarrollo y uso de los datos, previendo la participación de usuarios, la separación de entornos, la metodología a seguir, ciclos de vida y gestión, así como las consideraciones especiales respecto de aplicaciones y pruebas;

De cifrado.- Consiste en la implementación de algoritmos, claves, contraseñas, así como dispositivos concretos de protección que garanticen la integralidad y confidencialidad de la información; y

De comunicaciones y redes.- Se refiere a las restricciones preventivas y/o de riesgos que deberán observar los usuarios de datos o sistemas de datos personales para acceder a dominios o cargar programas autorizados, así como para el manejo de telecomunicaciones.

Niveles de seguridad:

Básico.- Se entenderá como tal, el relativo a las medidas generales de seguridad cuya aplicación es obligatoria para todos los sistemas de datos personales. Dichas medidas corresponden a los siguientes aspectos: documento de seguridad, funciones y obligaciones del personal que intervenga en el tratamiento de los sistemas de datos personales, registro de incidencias, Identificación y autenticación, control de acceso, gestión de soportes, y copias de respaldo y recuperación.

Correspondiendo a la siguiente clasificación los datos de:

a) Identificación
b) Laborales y seguridad social.

Medio.- Se refiere a la adopción de medidas de seguridad cuya aplicación corresponde a aquellos sistemas de datos relativos a la comisión de infracciones administrativas o penales, hacienda pública, servicios financieros, datos patrimoniales, así como a los sistemas que contengan datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo. Este nivel de seguridad, de manera adicional a las medidas calificadas como básicas, considera los siguientes aspectos: Responsable de seguridad, auditoria, control de acceso físico y pruebas con datos reales.

Corresponden a esta clasificación los datos:

a) Patrimoniales.
b) Sobre procedimientos administrativos en forma de juicio y/o jurisdiccionales.
c) Académicos y profesionales.
d) Tránsito y movimientos migratorios;

Alto.- Corresponde a las medidas de seguridad aplicables a sistemas de datos concernientes a distribución de soportes; registro de acceso; y telecomunicaciones.

Corresponden a esta clasificación los datos:

a) Ideológicos
b) Los relativos a la salud
c) Las Características personales
d) Las características físicas
e) La vida sexual
f) Origen racial o étnico

Las medidas de seguridad a las que se refiere el numeral anterior constituyen los mínimos exigibles, por lo que los Sujetos Obligados adoptarán las medidas adicionales que estimen necesarias para brindar mayores garantías en la protección y custodia de

los sistemas de datos personales. Por la naturaleza de la información, las medidas de seguridad que se adopten serán consideradas confidenciales y únicamente se comunicará al Instituto, para su registro, el nivel de seguridad aplicable.

Trigésimo noveno. Las especificaciones de cada uno de los niveles antes mencionados figuran en el instructivo para el llenado del formulario para la inscripción del Registro Estatal de Datos Personales, aprobados en esta misma fecha y que aparecen como (Anexo 1) de los presentes lineamientos. El formulario se llenará mecánica y electrónicamente.

Cuadragésimo. De acuerdo con sus facultades, atribuciones y finalidades cada sujeto obligado, clasificará los datos personales que obren en su poder dentro de las categorías mencionadas en el lineamiento anterior.

TÍTULO TERCERO
Capítulo VI

Del registro y sistema electrónico

Cuadragésimo primero. Es el Órgano del Instituto el cual tiene como objeto el control sobre la existencia y finalidad de los sistemas de datos personales en poder de los sujetos obligados.

Cuadragésimo segundo. El Registro Estatal de Protección de Datos Personal contará con un titular propuesto por el Comisionado Presidente y ratificado por el Pleno del Consejo General.

Facultades del titular.

Cuadragésimo tercero. El Registro Estatal de protección de Datos personales tendrá las siguientes facultades y deberes:

I. Inscribir los sistemas de datos personales de los sujetos obligados.
II. Recomendar sobre las medidas de seguridad de los sistemas de datos personales adoptados por los sujetos obligados.
III. Elaborar instructivos y formularios, a que se refiere el numeral Trigésimo noveno de los presentes lineamientos y los demás que establezca la ley.
IV. Coadyuvar con los sujetos obligados en la publicación de los sistemas de datos personales en el registro.
V. Responder, a través de la Unidad de Enlace del Instituto, a las solicitudes de información relacionadas con la existencia y finalidad de los sistemas de datos personales.
VI. Coadyuvar con las distintas áreas del Instituto en la supervisión, investigación, asesoría, capacitación y difusión en la materia.
VII. Expedir a los sujetos obligados, las constancias de inscripción de sus sistemas de datos personales al Registro.

VIII. Formular su programa de trabajo para integrarlo al Programa de Trabajo Institucional (PTI) del Instituto.
IX. Preparar el informe correspondiente a sus actividades conforme a lo dispuesto en el Plan de Trabajo Institucional.
X. Las demás que señale la ley.

Capítulo VII
Del Sistema Electrónico

Cuadragésimo cuarto. Para instituir el Registro Estatal de protección de Datos Personales, el Instituto pondrá a disposición de los sujetos obligados el Sistema electrónico Multimedia de Registro de Datos Personales. Mediante este sistema electrónico se incorporarán los formularios de censo e inscripción en línea.

Cuadragésimo quinto. Los Responsables deberán registrar e informar al Instituto a través del Registro Estatal de Protección de Datos Personales, dentro de los primeros diez días hábiles de enero y julio de cada año, lo siguiente:

a) Los sistemas de datos personales;
b) Normatividad aplicable al sistema.
c) La estructura básica del sistema de datos personales y la descripción de los tipos de datos incluidos en el mismo
d) El nivel de seguridad y protección que corresponde.
e) La finalidad del sistema de datos personales y los usos previstos
f) Las personas o grupos de personas sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.
g) El procedimiento de recolección de los datos de carácter personal.
h) Las instancias responsables del tratamiento del sistema de datos personales.
i) La unidad administrativa ante la que podrán ejercerse los derechos de acceso, rectificación, cancelación u oposición;
j) Cualquier creación, modificación, cancelación o baja de dichos sistemas,
k) Cualquier transmisión de sistemas de datos personales de conformidad a lo dispuesto por los Lineamientos Vigésimo tercero y Vigésimo cuarto de los presentes Lineamientos.

Lo anterior será incorporado al Sistema Electrónico Multimedia de Registro de Datos Personales, así como publicado en forma actualizada en las páginas electrónicas correspondientes a cada sujeto obligado.

Datos del registro

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

a) Indicar el nombre del responsable del sistema de datos personales.
b) Indicar el nombre asignado al sistema de datos personales.
c) Indicar fundamento legal en donde se les da facultades para recabar los datos personales.
d) Finalidades para los que fueron recabados los datos personales.
e) Nombre, teléfono y correo electrónico del responsable, encargados y usuarios.
f) Cargo del Responsable.
g) Datos de identificación de la unidad administrativa responsable de los datos personales.
h) Naturaleza y niveles de seguridad de los datos personales contenidos en cada sistema.
i) Forma de recolección y actualización de datos
j) Destino de los datos y personas físicas o morales a las que pueden ser transmitidos.
k) Describir finalidad de la transmisión.
l) Informar cualquier creación, modificación, cancelación o baja que se registre en dichos sistemas.
m) Medidas de seguridad adoptadas

Cuadragésimo séptimo. El Instituto otorgará al responsable un folio de registro por cada sistema de datos personales para su identificación.

Vínculo al Sistema Electrónico

Cuadragésimo octavo. Las dependencias y entidades deberán establecer un vínculo en sus sitios de Internet al Sistema Multimedia de Registro de Datos Personales, a efecto de dar a conocer el índice de sistemas de datos personales que poseen**.**

Capítulo VIII

De la supervisión por el Instituto

Supervisión de la Protección

Cuadragésimo noveno. Los sujetos obligados 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 física, técnica y administrativa de los mismos, a fin de supervisar que se cumpla con la Ley y los presentes Lineamientos.

Responsabilidades

Quincuagésimo. En caso de que el Instituto determine que algún servidor público pudo haber incurrido en responsabilidad por el incumplimiento de los presentes Lineamientos, lo hará del conocimiento del Órgano Interno de Control correspondiente, a efecto de que determine lo conducente, con base en el capítulo de Responsabilidades y Sanciones

establecido en el Capítulo IV de la Ley de Protección de Datos Personales, así como en la de Responsabilidades de los Servidores Públicos del Estado y Municipios de Oaxaca.

Transitorios

Primero. Los presentes Lineamientos entrarán en vigor al día siguiente de su publicación en la página electrónica del Instituto www.ieaip.org.mx.

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 implementados en términos del Lineamiento Décimo sexto, a más tardar el día 01 de abril de 2009.

Tercero. El cumplimiento de las disposiciones contenidas en el capítulo V de los presentes Lineamientos deberá efectuarse a más tardar en diciembre de 2009, incluido el documento de seguridad a que se refiere el Lineamiento Trigésimo segundo.

Cuarto. La primera actualización del Sistema Multimedia de Registro de Datos Personales por parte de los sujetos obligados a que se refiere el Lineamiento Cuadragésimo quinto, deberá llevarse a cabo dentro de los primeros diez días hábiles de julio de 2009.

Por única ocasión los informes correspondientes al mes de enero del presente año se excluyen del plazo contemplado en el numeral Cuadragésimo quinto, no así los correspondientes al mes de julio.

Quinto. Las primeras recomendaciones sobre las medidas de seguridad que se mencionan en el Lineamiento Trigésimo séptimo, serán emitidas por el Instituto a más tardar en el mes de junio de 2009.

Así lo acordó por unanimidad el Pleno del Instituto Estatal de Acceso a la Información Pública, en sesión celebrada el día catorce de enero de dos mil nueve. Publíquese de inmediato en la página electrónica www.ieaip.org.mx .- El Comisionado Presidente, **Genaro Víctor Vásquez Colmenares**.- Rúbrica.- Los Comisionados: **Alicia Aguilar Castro y Raúl Ávila Ortiz**.- Rúbricas.- El Secretario General, **Luis Antonio Ortiz Vásquez**.- Rúbrica.