EL ESTADO DE JALISCO
PERIÓDICO OFICIAL

JALISCO
GOBIERNO DEL ESTADO
PODER EJECUTIVO

SECRETARÍA GENERAL DE GOBIERNO

OFICIALÍA MAYOR DE GOBIERNO

DIRECCIÓN DE PUBLICACIONES

Registrado desde el
3 de septiembre de 1921.
Trisemanal:
martes, jueves y sábados.
Franqueo pagado.
Publicación Periódica.
Permiso Número 0080921.
Características 117252816.
Autorizado por SEPOMEX.

periodicooficial.jalisco.gob.mx

MARTES 10 DE JUNIO
DE 2014

GUADALAJARA, JALISCO
TOMO CCCLXXIX

EL
ESTADO DE JALISCO
PERIÓDICO OFICIAL

Registrado desde el
3 de septiembre de 1921.
Trisemanal:
martes, jueves y sábados.
Franqueo pagado.
Publicación Periódica.
Permiso Número 0080921.
Características 117252816.
Autorizado por SEPOMEX.

periodicooficial.jalisco.gob.mx

JALISCO
GOBIERNO DEL ESTADO

ACUERDO

Al margen un sello que dice: Instituto de Transparencia e Información Pública de Jalisco.

ACUERDO DEL CONSEJO DEL INSTITUTO DE TRANSPARENCIA E INFORMACION PÚBLICA DE JALISCO MEDIANTE EL CUAL SE EMITEN LOS LINEAMIENTOS GENERALES PARA LA PROTECCIÓN DE LA INFORMACIÓN CONFIDENCIAL Y RESERVADA QUE DEBERÁN OBSERVAR LOS SUJETOS OBLIGADOS PREVISTOS EN LA LEY DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA DEL ESTADO DE JALISCO Y SUS MUNICIPIOS.

El Pleno del Consejo del Instituto de Transparencia e Información Pública de Jalisco, con fundamento en los artículos 35 punto 1, fracción XII, inciso c, 41 punto 1, fracción VII, inciso c de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.

CONSIDERANDO

I. El artículo 6º de la Constitución Política del los Estados Unidos Mexicanos, determina que en el ejercicio del acceso a la información deben regir entre otros principios, el que se refiere a la vida privada y los datos personales, que serán protegidos en los términos y con las excepciones que fijan las leyes aplicables a la materia.

II. El artículo 16º Constitucional tras la reforma publicada el 01 de junio de 2009 dos mil nueve, reconoce el derecho de toda persona a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como su oposición en los términos que fijen las leyes, respetando los principios que rijan el tratamiento de datos personales, salvo las excepciones establecidas por razón de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

III. Dentro del ámbito internacional, tanto el artículo 12 de la Declaración Universal de los Derechos Humanos, como el artículo 5º de la Declaración Americana de los Derechos y Deberes del Hombre de 1948, protegen el derecho de la vida privada, así como la obligación de los Estados firmantes de garantizar esa protección en la legislación interna por medio de leyes, reglamentos y lineamientos.

IV. La Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, establece que este Instituto tiene entre sus funciones la de proteger la información pública reservada y confidencial, para lo cual tiene entre sus atribuciones emitir de acuerdo a estándares nacionales e internacionales y publicar en el Periódico Oficial "El Estado de Jalisco", los Lineamientos Generales para la Protección de la Información Confidencial y Reservada.

Por lo antes vertido, el Pleno del Consejo del Instituto de Transparencia e Información Pública de Jalisco, con el objeto de dar cumplimiento a la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, tiene a bien emitir los siguientes:

LINEAMIENTOS GENERALES PARA LA PROTECCIÓN DE LA INFORMACIÓN CONFIDENCIAL Y RESERVADA QUE DEBERÁN OBSERVAR LOS SUJETOS OBLIGADOS PREVISTOS EN LA LEY DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA DEL ESTADO DE JALISCO Y SUS MUNICIPIOS.

Capítulo I
Disposiciones Generales

PRIMERO: Los presentes Lineamientos tienen por objeto establecer los procedimientos que deberán observar los sujetos obligados para el debido manejo, mantenimiento, seguridad y protección de la información confidencial y reservada. Aunado a lo anterior, constituyen la base para la emisión de los criterios generales, que en lo particular deben publicar los sujetos obligados.

SEGUNDO: Para los efectos de los presentes Lineamientos se emplearán las definiciones contenidas en el artículo 4º de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios y las previstas por el artículo 2° de su Reglamento.

TERCERO: Los sujetos obligados deberán elaborar sus políticas en relación a la protección de la información confidencial y reservada que tengan en su poder, contra acceso, utilización, sustracción, modificación, destrucción y eliminación no autorizados.

CUARTO: Para los efectos de los presentes Lineamientos, se entenderá por protección, todo acto encaminado a asegurar el buen funcionamiento del manejo y

seguridad de la información, que garantice la no revelación de la información confidencial y reservada que obre en poder de los sujetos obligados.

QUINTO: Por información Reservada se entiende la señalada en el artículo 17 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, e Información Confidencial la referida en el artículo 21 del mismo ordenamiento.

SEXTO: Los servidores públicos que con motivo de sus labores, tengan a su alcance información confidencial o reservada, deberán guardar el secreto profesional respecto a la misma, aun después de concluida su gestión y/o contratación. Lo mismo aplica con las personas que sean contratadas por los sujetos obligados bajo cualquier otro régimen.

SÉPTIMO: Los sujetos obligados no podrán comercializar, distribuir o difundir información confidencial contenida en los sistemas y documentos desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso y por escrito del titular de dicha información, de conformidad con el artículo 23 punto 1, fracción IV de la Ley.

OCTAVO: Todos los sujetos obligados, al momento de elaborar sus actas de entrega y recepción al término de sus funciones, deberán incluir un apartado especial en el que se especifiquen los documentos y/o soporte digital o magnético que contiene la información de carácter confidencial.

Capítulo II
Protección de la Información Confidencial y Reservada

Sección I
De la Información Reservada

NOVENO: Para dictaminar si la información tiene el carácter de reservada los sujetos obligados a través de su comité de Clasificación, deberán determinar que la misma se encuentra dentro de los supuestos que prevé el artículo 17 de la Ley, además de precisar que la publicidad de la misma causaría un daño presente, probable y específico.

DÉCIMO: La información reservada únicamente deberá ser manejada por el personal directamente involucrado en las labores propias de la generación y manejo de la información.

DÉCIMO PRIMERO: La información que tenga el carácter de reservada deberá ser resguardada en un lugar seguro, de manera que no se conserve en archivos de fácil acceso al público.

DÉCIMO SEGUNDO: El Instituto, podrá tener acceso a la información reservada, así como a la inspección y vigilancia de los esquemas de mantenimiento o aseguramiento que fijen los sujetos obligados en sus criterios generales.

DÉCIMO TERCERO: Para negar el acceso a la información reservada, los sujetos obligados deben justificar que se cumpla lo siguiente:

I. Que la información solicitada se encuentra prevista en alguna hipótesis de reserva y/o confidencial que establece la ley.
II. Que la revelación de dicha información atente efectivamente el interés público protegido por ley.
III. Que el daño o perjuicio que se produce con la revelación de la información es mayor que el interés público de conocer la información de referencia

Para dar cumplimiento a lo anterior, el Comité de Clasificación deberá acreditar mediante la prueba de daño que se actualizan los tres supuestos señalados, y cuyo resultado se asentará en un acta.

DÉCIMO CUARTO: Para el supuesto en que los documentos contengan parcialmente información reservada, los sujetos obligados deberán expedir una versión pública, en la que se supriman los datos reservados, señalando los fundamentos y motivaciones de esta restricción informativa.

Sección II
De la Información Confidencial

DÉCIMO QUINTO: Es Información Confidencial la referida en los articulos 4 punto 1 fracción IV y V, 20 y 21 de la Ley.

A efecto de determinar si la información que posea cualquier sujeto obligado se trata de información confidencial, deberán considerarse las siguientes hipótesis:

a) Que la misma sea concerniente a una persona física, identificada o identificable, debiendo entenderse como identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, y que en razón de su contenido permite acceder al conocimiento de diversos aspectos de la persona, incluso obtener una imagen diversificada y compleja de la misma, apta para establecer perfiles de categorización a través de múltiples operaciones de tratamiento a que puedan ser sometidos, que puedan vincularse entre sí, afectando los datos más frágiles y vulnerables en la esfera del ser humano, a través de la exhibición pública y de la incursión sin consentimiento previo a la vida intima y familiar.

b) Que los datos de una persona se encuentra contenida en sus archivos y que la misma constituye una asociación entre la información y la persona.

DÉCIMO SEXTO: Además de la información referida en el artículo anterior, se clasificará como información confidencial, aquella referente a las personas jurídicas, concerniente al estado económico, comercial o la relativa a su identidad que de revelarse, pudiera anular o menoscabar su libre y buen desarrollo.

DÉCIMO SÉPTIMO: Los bienes protegidos por el derecho de protección relativos a las personas jurídicas, comprenden aquellos documentos e información que les son inherentes, que deben permanecer ajenas al conocimiento de terceros, como lo son aquellos que contengan datos relativos a los estados financieros, cuentas bancarias e información fiscal y contable.

DÉCIMO OCTAVO: Cuando se solicite información relativa a los datos personales, en todo caso podrá ser proporcionada, si se lleva a cabo el procedimiento de disociación.

La disociación consiste en el procedimiento por el cual, los datos personales no pueden asociarse a su titular, ni permitir, por su estructura, contenido o grado de difusión, la identificación individual del mismo.

DÉCIMO NOVENO: Cuando un sujeto obligado reciba información que tenga el carácter de confidencial, este deberá hacer del conocimiento de la persona física o jurídica que entregue dicha información, la existencia del aviso de confidencialidad que establece el reglamento de la Ley de la materia.

VIGÉSIMO: Los datos personales son irrenunciables, intransferibles e indelegables, por lo que no podrán transmitirse salvo disposición legal o cuando medie el consentimiento del titular y dicha obligación subsistirá aún después de finalizada la relación entre el ente público con el titular de los datos personales, así como después de finalizada la relación laboral entre el ente público y el responsable del sistema de información confidencial o los usuarios.

En caso de que fallecimiento del titular de los datos personales, se sujetara a lo previsto por los artículos 17 y 18 del Reglamento.

VIGÉSIMO PRIMERO: En el tratamiento particularmente de los datos personales, los sujetos obligados deberán observar los principios de licitud, confidencialidad consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, así como las medidas necesarias para el manejo, mantenimiento, seguridad y protección de dicha información.

VIGÉSIMO SEGUNDO: Por principio de licitud se entenderá toda aquella recolección de datos personales que se realice a través de los medios legales o reglamentarios de cada sujeto obligado previsto para tales efectos.

VIGÉSIMO TERCERO: El principio de confidencialidad, consiste en garantizar que exclusivamente la persona interesada puede acceder a los datos personales o, en su caso, el responsable o el usuario del sistema de información confidencial para su tratamiento, así como el deber de secrecía del responsable del sistema de información confidencial, así como de los terceros responsables.

VIGÉSIMO CUARTO: El principio de consentimiento, se refiere a la manifestación de voluntad libre, inequívoca, específica e informada, mediante la cual el interesado consiente el tratamiento de sus datos personales.

VIGÉSIMO QUINTO: Toda transmisión de datos personales deberá contar con el consentimiento del Titular de los datos, mismo que deberá otorgarse en forma libre, expresa e informada, salvo lo dispuesto en el artículo 22 de la Ley.

Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, y/o firma electrónica.

VIGÉSIMO SEXTO: El principio de información, consiste en hacer del conocimiento del Titular de los datos, al momento de recabarlos y de forma

escrita, el fundamento y motivo de ello, así como finalidades y usos para los cuales se tratarán dichos datos.

Los sujetos obligados que recaben datos personales a través de un servicio de orientación telefónica, u otros medios, deberán informar verbalmente a sus titulares la existencia del aviso de confidencialidad

VIGÉSIMO SÉPTIMO: Por principio de calidad de los datos personales, se entiende que el tratamiento de dichos datos deberá ser exacto, adecuado, pertinente y no excesivo, respecto de las atribuciones legales que el sujeto obligado posea.

VIGÉSIMO OCTAVO: A efecto de cumplir con el principio de calidad a que se refiere el lineamiento que antecede, 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 pueda traer como consecuencia que el titular de los datos se vea afectado por dicha situación;
b) Adecuado: Cuando se observan la medidas 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 hubiera recabado.

VIGÉSIMO NOVENO: Para efectos de cumplir con el lineamiento que precede, los sujetos obligados podrán implementar en la recolección de dicha información, formatos que contengan como requisitos mínimos los señalados anteriormente.

TRIGÉSIMO: El Principio de Finalidad, consiste en que los datos personales recabados por los sujetos obligados deberán ser tratados exclusivamente para la finalidad que fueron obtenidos.

TRIGÉSIMO PRIMERO: Los servidores públicos que por el desempeño de sus labores deben recolectar datos personales, deberán guiarse por el Principio de Lealtad, que consiste en la prohibición de recolectar datos en forma contraria a la Ley o por medios fraudulentos, desleales o ilícitos.

TRIGÉSIMO SEGUNDO: Los sujetos obligados, en el tratamiento de datos personales, deberán apegarse al Principio de Proporcionalidad, para lo cual deben asegurarse que los datos personales solicitados estén relacionados con los propósitos para los cuales fueron recolectados.

TRIGÉSIMO TERCERO: Los servidores públicos que en el desempeño de sus labores tengan contacto con datos personales, tienen que actuar de conformidad al Principio de Responsabilidad, y dar cumplimiento a las medidas de seguridad que se adopten en la protección de la Información Confidencial.

TRIGÉSIMO CUARTO: Los datos personales deberán ingresarse en un sistema de información confidencial previamente diseñado conforme a la naturaleza de los datos, su finalidad y los usos previstos para el mismo, de forma tal, que los datos personales, sean identificables y permitan el ejercicio de los derechos de acceso, rectificación, modificación, corrección, sustitución, oposición, supresión o ampliación de datos de la información confidencial previstos por la Ley.

TRIGÉSIMO QUINTO: Los instrumentos jurídicos que correspondan a la contratación de servicios del responsable del sistema de información confidencial, así como de los terceros responsables, deberán prever la obligación de garantizar la seguridad y confidencialidad de esos sistemas, así como la prohibición de utilizarlos con propósitos distintos para los cuales se llevó a cabo la contratación, además se establecerán las penas convencionales por su incumplimiento. Lo anterior, sin perjuicio de las responsabilidades previstas en otras disposiciones aplicables.

TRIGÉSIMO SEXTO: Los datos personales, que hayan sido obtenidos para un fin particular agotado y que su conservación resulte innecesaria, deberán ser eliminados del sistema al que pertenezcan; y en caso de tratarse de documentos físicos, tales como expedientes, se apegará al proceso de depuración previsto por los artículos 15 y 16 de la Ley que regula la Administración de Documentos Públicos e Históricos del Estado de Jalisco, para ambos supuestos se levantara constancia y/o previo recibo de entrega a su titular.

TRIGÉSIMO SÉPTIMO: Los sujetos obligados deberán generar el conjunto de actividades y medidas necesarias para asegurar el buen funcionamiento del manejo, seguridad y protección de la información confidencial y reservada.

CAPÍTULO III
DISPOSICIONES COMUNES PARA LA SEGURIDAD DE LA INFORMACIÓN CONFIDENCIAL Y RESERVADA

TRIGÉSIMO OCTAVO: Las medidas de seguridad que implementen los sujetos obligados, deberán ser las suficientes para garantizar la integridad, confiabilidad, confidencialidad y disponibilidad de la información protegida mediante acciones que eviten la alteración, perdida, trasmisión y acceso no autorizado, de conformidad a la Ley, su Reglamento y los presentes Lineamientos.

TRIGÉSIMO NOVENO: Las medidas de seguridad que podrán emplear los sujetos obligados para garantizar la seguridad de la información confidencial y reservada, se realizarán tomando en consideración los tipos y niveles de seguridad que requiere la información que posee.

CUADRAGÉSIMO: Para los efectos del artículo que precede son tipos de seguridad:

I. Física.- Se refiere a toda medida orientada a la protección de instalaciones, equipos, soportes o sistemas de información confidencial o reservada para la prevención de riesgos por caso fortuito o causas de fuerza mayor.

II. Lógica.- Se refiere a las medidas de protección que permiten la identificación y autentificación de las personas o terceros responsables, autorizados para el tratamiento de la información confidencial y reservada de acuerdo con su función.

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

IV. 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.

V. De comunicaciones y redes.- Se refiere a las restricciones preventivas y/o de riesgos que deberán observar los servidores públicos que usen datos o sistemas

de información confidencial para acceder a dominios o cargar programas autorizados, así como para el manejo de telecomunicaciones.

CUADREGÉSIMO PRIMERO: Son niveles de seguridad, los que se describe a continuación:

I. Básico.- Se entenderá como tal, el relativo a las medidas generales de seguridad cuya aplicación es obligatoria para todos los sistemas de información confidencial. Dichas medidas corresponden a los siguientes aspectos:

a) Documento de seguridad;
b) Funciones y obligaciones del personal que intervenga en el tratamiento de los sistemas de datos personales;
c) Registro de incidencias;
d) Identificación y autentificación;
e) Control de acceso;
f) Gestión de soportes, y
g) Copias de respaldo y recuperación.

II. Medio.- Se refiere a la adopción de medidas de seguridad cuya aplicación corresponde a aquellos sistemas 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:

a) Responsable de seguridad;
b) Auditoria;
c) Control de acceso físico; y
d) Pruebas con datos reales.

III. Alto.- Corresponde a las medidas de seguridad aplicables a sistemas de información confidencial concernientes a la ideología, religión, creencias, afiliación política, origen racial o étnico, salud, biométricos, genéticos o vida sexual, así como los que contengan datos recabados para fines policiales, de seguridad, prevención, investigación y persecución de delitos. Los sistemas de información confidencial a los que corresponde adoptar el nivel de seguridad alto, además de incorporar las medidas de nivel básico y medio, deberán completar las que se detallan a continuación:

a) Distribución de soportes;
b) Registro de acceso; y
c) Telecomunicaciones.

Los diferentes niveles de seguridad serán establecidos atendiendo a las características propias de la información.

Estas medidas de seguridad constituyen mínimos exigibles, por lo que el sujeto obligado adoptará las medidas adicionales que estime necesarias para brindar mayores garantías en la protección y resguardo de los sistemas de información confidencial y de la información clasificada como reservada.

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.

CUADRAGÉSIMO SEGUNDO: Cuando se remita información confidencial a otros sujetos obligados, para el ejercicio de sus facultades, ajustado a lo previsto en las fracciones VI y VII del artículo 22 de la Ley, deberá informarse las medidas de seguridad o en su defecto, otras que se consideren pertinentes, con la finalidad de no afectar la confidencialidad o reserva de la información.

CUADRAGÉSIMO TERCERO: En caso de transferencia de información protegida, el responsable de dicha información deberá asegurarse que cuenta al menos con las medidas de protección siguientes:

a) Se incluya una carátula al inicio del documento, con la leyenda relativa al tipo de información que contenga, así como el nombre y cargo del destinatario.
b) En caso de tratarse de un documento electrónico deberá remitirse en un formato de archivo que no permita su edición o manipulación y deberá estar protegido de origen contra impresión o copiado no autorizado, parcial o total, de su contenido.
c) Se utilizarán mecanismos que aseguren que la información únicamente será tratada por el destinatario autorizado a recibirla.
d) Comunicar a los destinatarios sobre la responsabilidad que éstos adquieren al recibir la información a que se refiere este artículo.

e) Contenerse en sobre cerrado y sellado, cuyo traslado será a cargo de servidores públicos del sujeto obligado autorizado para ello.
f) Las demás medidas de protección que, de acuerdo a los riesgos y amenazas, el sujeto obligado considere necesario adoptar.

CUADRAGÉSIMO CUARTO: Los responsables de recibir la información confidencial y/o reservada que se transfiere, estarán obligados a:

1) Firmar el acuse de recibo correspondiente, haciendo constar hora y fecha de recepción, así como la integridad del sobre recibido, registrando al efecto, que no existan indicios de violación o cualquier otra irregularidad.
2) Mantener resguardada la información en área cerrada y dentro de mobiliario provisto de cerradura, caja de seguridad o estructura de seguridad equivalente, y
3) Abstenerse de efectuar reproducciones totales o parciales de la información recibida.
4) Realizar las acciones necesarias para contener la circulación de dicha información.

CUADRAGÉSIMO QUINTO: Para la protección de la información confidencial, los sujetos obligados, a través del encargado y/o responsable, podrán adoptar, dependiendo del material o soporte en el que se encuentre la información, las siguientes medidas administrativas, físicas y técnicas de seguridad:

I. Dar a conocer los presentes Lineamientos, así como la normatividad relativa al manejo, mantenimiento, seguridad y protección de la información confidencial, al personal del sujeto obligado;
II. Asignar un espacio físico seguro y adecuado para la operación de los sistemas de información confidencial, documentos u otro material en el que se encuentre la misma;
III. Llevar a cabo verificaciones periódicas de la correcta aplicación de las medidas de seguridad que se hayan decidido implementar;
IV. Controlar el acceso a las instalaciones o áreas, donde se encuentra el equipo o el material que soporta información confidencial, llevando un registro de las personas que acceden a ella;
V. Implementación de algoritmos, claves, contraseñas, códigos o candados

para el acceso directo a la información confidencial;
VI. Realizar respaldos que permitan garantizar la información confidencial, cuando se encuentre en medios magnéticos o digitales;
VII. Realizar las pruebas de las medidas de seguridad que se consideren aplicables, utilizando en paralelo copia de los datos reales, misma que deberá destruirse al final de la prueba;
VIII. Implementar otras medidas de seguridad para el uso de los dispositivos electrónicos y físicos que contengan información confidencial, para evitar el retiro no autorizado de los mismos; y
IX. Llevar un registro de incidencias de las fallas en las medidas de seguridad implementadas;

CUADRAGÉSIMO SEXTO: Los sujetos obligados podrán implementar otras medidas adicionales que según su normativa, organización y operatividad se adecuen, siempre con la finalidad de proteger la información confidencial.

CUADRAGÉSIMO SÉPTIMO: Las medidas de seguridad que los sujetos obligados adopten, serán considerando el presupuesto con el que se cuente, procurando el mayor grado de protección que amerite la información de que se trate, debiendo prestar mayor atención a los datos personales sensibles.

CUADRAGÉSIMO OCTAVO: Los sujetos obligados podrán expedir un documento, de seguridad; el que contemplará las medidas administrativas, físicas y técnicas de seguridad aplicables a la información confidencial, particularmente a los datos personales, según las necesidades de cada soporte o material en el que se encuentre la misma.

CUADRAGÉSIMO NOVENO: El documento mencionado en el Lineamiento anterior, deberá actualizarse periódicamente, según los cambios que lo ameriten y de conformidad con las políticas que en relación a la protección de datos emitan los sujetos obligados, mismo que deberá contener lo siguiente:

I. El nombre, cargo y adscripción del encargado y/o responsable)
II. Estructura y descripción de los sistemas y archivos en que se encuentra información confidencial;
III. Especificación del tipo de información confidencial;
IV. Funciones y obligaciones del personal autorizado para acceder a la información confidencial;
V. Medidas, normas, procedimientos y criterios enfocados a garantizar el nivel de seguridad exigido en los presentes lineamientos, los

cuales deberán:

a) Establecer los procedimientos para generar, asignar, distribuir, modificar, almacenar, dar de baja y alta a usuarios y claves de acceso para la operación de los sistemas de datos personales.
b) Procedimientos de creación de copias de respaldo y de recuperación de datos;
c) Procedimiento de notificación, gestión y respuesta ante incidentes respecto a las medidas de seguridad implementadas; y
d) Registro de cambios de las medidas de seguridad implementadas.

Capítulo IV
De los Responsables

QUINCUAGÉSIMO: Para el cumplimiento de los presentes Lineamientos el Comité de Clasificación, deberá designar a los servidores públicos que desarrollaran las funciones siguientes:

Responsable: Es el servidor público de la unidad administrativa a la que se encuentre adscrito el sistema de información confidencial, designado por el titular del ente público, que decide sobre el tratamiento de datos personales, así como el contenido y finalidad de los sistemas de información confidencial.

Encargado: Son los servidores públicos que en ejercicio de sus atribuciones realicen tratamiento de datos personales de forma cotidiana.

Tercero responsable: La persona física o moral, nacional o extranjera distinta del titular o del responsable de los datos, al que se transfieren los datos personales y que a su vez es responsable del tratamiento que les de.

QUINCUAGÉSIMO PRIMERO: Cualquiera de los antes descritos para resguardar información confidencial y/o reservada, podrán:

a) Adoptar las medidas de seguridad acordadas por el Comité, para el resguardo de los sistemas o documentos que contengan información

confidencial, mantenimiento y protección de la información confidencial y reservada, de manera que se evite su alteración pérdida o acceso no autorizado, pudiendo auxiliarse del personal que éste autorice para ello.

b) Llevar un registro permanentemente actualizado de las personas que tengan acceso a los sistemas o documentos que contengan información confidencial y reservada.

d) Hacer del conocimiento del Instituto, a través de su Comité de Clasificación los sistemas de información confidencial con que cuenten.

Capítulo V
De los Sistemas de Información Reservada y de Información Confidencial.

QUINCUAGÉSIMO SEGUNDO: Para dar cumplimiento a lo dispuesto por el artículo 35 punto 1, fracción XI de la Ley, los sujetos obligados deberán contar con un Sistema de Información Reservada y un Sistema de Información Confidencial.

QUINCUAGÉSIMO TERCERO: Los sujetos obligados deberán registrar e informar al Instituto, según corresponda, lo establecido en el Capitulo Segundo, Sección Segunda de la Ley; para lo cual el Instituto desarrollara una aplicación que permita mantener actualizado el listado de sistemas que cada sujeto obligado maneje.

QUINCUAGÉSIMO CUARTO: Los sujetos obligados deberán inscribirlos en el Registro habilitado por el Instituto, en un plazo no mayor a los 10 días hábiles siguientes a la creación del mismo.

Los sujetos obligados podrá elaborar un acuerdo de creación para los Sistemas de Información Confidencial y de Información Reservada y en la exposición considerativa deberá expresar la fundamentación y motivación correspondiente, así como cumplir con los requisitos previstos por la Ley y el Reglamento.

QUINCUAGÉSIMO QUINTO: En el acuerdo de creación de los Sistemas de Información Reservada, los sujetos obligados deberán tomar en consideración los datos que se enlistan a continuación:

I. EL acta de clasificación sobre la cual se pueda identificar el rubro temático de la información reservada que se trate.
II. Unidad administrativa que generó, obtuvo, adquirió, o conserva la información.
III. Fecha de clasificación que se refiere al día, mes y año, en el cual fue aprobada el acta de clasificación.
IV. La fundamentación legal sobre la cual se pretende sustentar el acto de clasificar la información como reservada.
V. El lapso de tiempo sobre el cual se reservara la información, especificando por evento o por la denominación de documento.
VI. En su caso, las partes del documento que se consideran como reservadas.

QUINCUAGÉSIMO SEXTO: Para el acuerdo de creación de un Sistema de Información confidencial se deberá establecer:

I. El aviso de confidencialidad que de manera general pondrá a disposición de los titulares de la información

II. En el caso del Sistema de Información Confidencial, los sujetos obligados deberán tomar en cuenta que la finalidad es el propósito legal para la recopilación de la información personal y el uso previsto, se refiere al empleo o destino que se le da a los datos personales obtenidos.

III. El origen de la Información Confidencial, así como el grupo de interesados al que va dirigido, es decir la procedencia o mecanismo por el que se obtienen la Información Confidencial o la Reservada (propio interesado, representante, ente público, etcétera), así como la indicación de la denominación del grupo o sector del que se realice la obtención, manejo o tratamiento de dicha información, o que resulten obligados a suministrarlos.

IV. El procedimiento de recopilación de la Información Confidencial, deberá indicar la forma o mecanismo de obtención de la misma (formulario, Internet, transmisión electrónica, etcétera).

V. La estructura básica de los Sistemas de Información Confidencial, es decir la descripción detallada de los datos que contiene cada sistema.

VI. Las cesiones de datos que se tengan previstas por la legislación aplicable a la materia entendiendo por cesión, toda obtención de datos resultante de la consulta de un archivo, registro, base o banco de datos, una publicación de los datos contenidos en él, su interconexión con otros ficheros y la comunicación de datos

realizada por una persona distinta a la interesada, así como la transferencia o comunicación de datos realizada entre entes públicos.

VII. La identificación del sujeto responsable, así como del responsable y sus encargados.

VIII. Indicación del nivel de seguridad que resulte aplicable, básico, medio o alto.

QUINCUAGÉSIMO SÉPTIMO: Los sistemas de información confidencial se distinguen en:

I. Físicos: Conjunto ordenado de datos de carácter personal que para su tratamiento están contenidos en registros manuales, impresos, sonoros, magnéticos, visuales u holográficos, estructurado conforme a criterios específicos relativos a personas físicas que permitan acceder sin esfuerzos desproporcionados a sus datos personales; y

II. Automatizados: Conjunto ordenado de datos de carácter personal que permita acceder a la información relativa a una persona física utilizado una herramienta tecnológica.

QUINCUAGÉSIMO OCTAVO: Para efectos de los presentes lineamientos, los datos personales que contengan el Sistema de información confidencial, se clasificarán, de manera enunciativa, más no limitativa, de acuerdo a las siguientes categorías:

I. Datos identificativos: El nombre, domicilio, teléfono particular, teléfono celular, firma, clave de Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), Clave de Elector, Matrícula del Servicio Militar Nacional, número de pasaporte, lugar y fecha de nacimiento, nacionalidad, edad, fotografía y demás análogos.
II. Datos de origen: Documentos que contengan datos referentes al origen étnico o racial.
III. Datos ideológicos: Son aquellos referentes a la ideología u opinión política, opinión pública, afiliación sindical y creencia o convicción religiosa y filosófica.
IV. Datos sobre la salud: El expediente clínico de cualquier atención médica, referencias o descripción de sintomatologías, detección de enfermedades, incapacidades médicas, discapacidades, intervenciones quirúrgicas, vacunas, consumo de estupefacientes, uso de aparatos oftalmológicos, ortopédicos,

auditivos, prótesis, estado físico o mental de la persona, así como la información sobre la vida sexual.
V. Datos Laborales: Documentos de reclutamiento y selección, nombramiento, incidencia, capacitación, actividades extracurriculares, referencias laborales, referencias personales, solicitud de empleo, hoja de servicio y demás análogos.
VI. Datos patrimoniales: Los correspondientes a bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, fianzas, servicios contratados, referencias personales y demás análogos.
VII. Datos sobre procedimientos administrativos y/o jurisdiccionales: La información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal, fiscal, administrativa o de cualquier otra rama del Derecho.
VIII. Datos académicos: Trayectoria educativa, calificaciones, títulos, cédula profesional, certificados y reconocimientos y demás análogos.
IX. Datos de tránsito y movimientos migratorios: Información relativa al tránsito de las personas dentro y fuera del país, así como información migratoria.

QUINCUAGÉSIMO NOVENO: El Instituto podrá emitir recomendaciones sobre los estándares mínimos de seguridad, de la información confidencial y reservada aplicables a los sistemas, documentos u en otro material en que se encuentre dicha información esto, en función a la vigilancia del cumplimiento de las disposiciones de la Ley

SEXUAGÉSIMO: El responsable del sistema de información confidencial o los usuarios podrán ser relevados del deber de confidencialidad por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la seguridad nacional o la salud pública.

TRANSITORIOS

PRIMERO.- Los presentes Lineamientos entrarán en vigor al día siguiente de su publicación en el Periódico Oficial "El Estado de Jalisco".

SEGUNDO.- Los presentes Lineamientos deberán ser publicados en el sitio de Internet del Instituto, y en los medios que se estime pertinente.

TERCERO.- Como consecuencia de la expedición de los presente Lineamientos, quedan sin efecto los emitidos por el Consejo en años anteriores que tengan relación con los temas expuestos en los presentes.

Guadalajara, Jalisco a 28 veintiocho de mayo de 2014 dos mil catorce. Se aprobaron los presentes Lineamientos Generales para la Protección de la Información Confidencial y Reservada, que deberán observar los sujetos obligados previstos en el artículo 24 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.

Así lo acordó el Consejo del Instituto de Transparencia e Información Pública de Jalisco, en la Décimo Octava sesión ordinaria, ante el Secretario Ejecutivo quien certifica y da fe.

Cynthia Patricia Cantero Pacheco.
Presidenta del Consejo

Francisco Javier González Vallejo
Consejero Titular

Pedro Vicente Viveros Reyes
Consejero Titular

Miguel Ángel Hernández Velázquez.
Secretario Ejecutivo