CRITERIOS GENERALES EN MATERIA DE PROTECCIÓN DE LA INFORMACIÓN CONFIDENCIAL Y RESERVADA DEL INSTITUTO DE TRANSPARENCIA E INFORMACIÓN DE JALISCO.

El Comité de Clasificación de Información Pública del Instituto de Transparencia e Información Pública de Jalisco, con fundamento en los artículos 24, punto 1, fracción XI, 25, numeral 1, fracción IX, inciso c), de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; así como la fracción II, del numeral 6 del Reglamento de la Ley, tiene la atribución de emitir los Criterios Generales en Materia de Publicación y Actualización de Información Fundamental, lo que se efectúa al tenor de los siguientes:

CONSIDERANDOS

I. El derecho a la protección de datos personales debe ser garantizado por el Estado, ya que es un derecho fundamental protegido por la legislación mexicana, Tratados y Convenios Internacionales en la materia, además de ser un derecho de última generación.

En el marco normativo mexicano se prevé que el derecho de protección de datos personales es un derecho humano fundamental, por su parte, los artículos 6 y 16 constitucionales establecen los principios y bases en los cuales habrá de estar sustentado el ejercicio del derecho, además de señalar los límites de acceso a la información en razón de proteger la vida privada, el interés público y los datos personales, así como señalar que todas las personas tienen derecho a la protección, al acceso, rectificación y cancelación de los mismos.

II.- En tal contexto, el Instituto de Transparencia e Información Pública de Jalisco, es el órgano encargado de dar cumplimiento a dicha función, de conformidad con los principios rectores de máxima publicidad de este derecho, además de cumplir con los principios de gratuidad, interés general, libre acceso, mínima formalidad, sencillez y celeridad, suplencia de la deficiencia y transparencia.

III.- El artículo 25 punto 1, fracción IX, inciso c) de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, establece que es obligación de este sujeto obligado emitir y publicar de acuerdo a los Lineamientos

Generales que emita el Instituto, su Criterios Generales en Materia de Protección de Información Confidencial y Reservada.

En razón de lo antes expuesto el Comité de Clasificación del Instituto de Transparencia e Información Pública de Jalisco emite los siguientes

CRITERIOS GENERALES EN MATERIA DE PROTECCIÓN DE LA INFORMACIÓN CONFIDENCIAL Y RESERVADA DEL INSTITUTO DE TRANSPARENCIA E INFORMACIÓN DE JALISCO.

CAPÍTULO I
Disposiciones Generales

PRIMERO: Los presentes criterios tienen por objeto determinar las directrices a seguir en el tratamiento que se dará a la información confidencial y reservada, constituyendo las bases que establecen los procedimientos que se observarán para el debido manejo, mantenimiento, seguridad y protección de la misma.

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

TERCERO: Para los efectos de los presentes criterios se entiende 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.

CUARTO: Los servidores públicos de este Instituto 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 bajo cualquier otro régimen.

QUINTO: De conformidad con el artículo 23 punto 1, fracción IV de la Ley, este Instituto no puede comercializar, distribuir o difundir la información confidencial contenida en los sistemas de información reservada y confidencial, y en documentos desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso y por escrito del titular de dicha información.

CAPÍTULO II
Protección de la Información Confidencial y Reservada
Sección I
De la Información Reservada

SEXTO: Es información Reservada aquella que cumpla con los requisitos previstos por el artículo 17 de la Ley, misma que será objeto de clasificación por parte del Comité de Clasificación de este Instituto.

SÉPTIMO: En el acta de clasificación que se emita derivada de la sesión del Comité de Clasificación en la que se realizó, deberá establecerse el plazo de reserva, que no podrá exceder de seis años. En el caso de tratarse de una ampliación al tiempo de reserva, debe estar fundada y motivada.

OCTAVO: La información reservada solo será manejada por el personal del Instituto que, por las actividades que desempeña, se encuentra involucrado en las labores propias de su generación y tratamiento.

NOVENO: La información que tenga el carácter de reservada debe encontrarse en un lugar seguro, con acceso restringido al público.

DÉCIMO: Tratándose de documentos que contengan parcialmente información reservada, deberá elaborarse la versión pública del mismo, en la que se supriman los datos reservados, señalando los fundamentos y motivaciones de la restricción informativa.

DÉCIMO PRIMERO: El Comité de Clasificación tiene la obligación de establecer el Sistema de Información Reservada, además de informar al Instituto de la existencia del mismo, dentro de los diez días hábiles siguientes a su emisión, lo que dará inicio a procedimiento de reconocimiento del Sistema de Información Reservada, de acuerdo al artículo 47 fracción I del Reglamento.

Sección II

De la Información Confidencial

DÉCIMO SEGUNDO: Es información confidencial la prevista por el artículo 21 de la Ley, por lo que únicamente podrá ser transferida sin el consentimiento de su titular en los supuestos previstos por el artículo 22 de la Ley.

DÉCIMO TERCERO: Cuando este Instituto reciba información con el carácter de confidencial, se hará saber al titular de la misma los derechos que puede ejercer previstos por la Ley y su Reglamento.

DÉCIMO CUARTO: Además de lo previsto en el criterio anterior, el Comité de Clasificación debe verificar que la información entregada como confidencial cumple con lo establecido por el artículo 21 punto 1, fracciones I y II de la Ley, cerciorándose que pertenece a una persona física, identificada o identificable, debiendo entenderse como identificable toda persona cuya identidad pueda determinarse directa o indirectamente; que esos datos se encuentren en sus archivos y que se pueda dar una asociación entre la información y la persona.

DÉCIMO QUINTO: En caso de que a este Instituto ingrese información correspondiente a personas jurídicas, como documentos y datos relativos a los estados financieros, cuentas bancarias e información fiscal y contable, se analizará si debe clasificarse como información confidencial, para lo cual se considerará si la

difusión de la misma causa perjuicio al estado económico, comercial o a su identidad.

DECIMO SEXTO: Para poder entregar información que contenga datos personales, primero se tendrá que realizar el proceso de disociación, es decir, se analizará que los datos personales no puedan ser asociados o permitan, por su estructura, grado o contenido de difusión, identificar al individuo del que se trate.

DÉCIMO SÉPTIMO: Este Instituto contará con un aviso de confidencialidad, que se dará a conocer a los titulares de los datos personales al momento de recibir información con ese carácter.

DÉCIMO OCTAVO: Una vez que se reciban en este Instituto datos personales, se les dará tratamiento bajo los principios de licitud, confidencialidad, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, y se tomarán las medidas de seguridad y protección de dicha información.

Para la interpretación y aplicación de los principios citados en el párrafo que antecede, se apegará a las definiciones que se describen en los Lineamientos Generales para la Protección de la Información Confidencial y Reservada, publicados en el Periódico Oficial "El Estado de Jalisco" el 10 diez de junio del 2014 dos mil catorce.

DÉCIMO NOVENO: El Instituto contará con un Sistema de Información Confidencial, que contendrá la siguiente información:

a) Naturaleza de los datos (personales y/ personales sensibles).
b) Finalidad y los usos previstos para los datos.
c) Proceso de recopilación de la información.
d) La estructura del sistema.
e) Cesión de datos personales.
f) La identificación del Instituto y de los servidores públicos responsables y de los encargados.

g) Nivel de seguridad.

CAPÍTULO III
MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN CONFIDENCIAL Y RESERVADA

VIGÉSIMO: Para la protección de la información confidencial y reservada este Instituto deberá establecer, de acuerdo con su presupuesto y tomando en consideración la naturaleza de la misma, las medidas de seguridad que considere pertinentes.

VIGÉSIMO PRIMERO: Las medidas de seguridad se clasifican en tres niveles: básico, medio y alto, los cuales se establecen atendiendo a la naturaleza de la información tratada, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información.

VIGÉSIMO SEGUNDO: Para la aplicación de los niveles de seguridad se tomará en cuenta lo siguiente:

a) Los documentos que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como de nivel básico.
b) Aquellos documentos y datos relativos a la comisión de infracciones administrativas o penales, datos financieros, tendrán además del nivel básico el considerado como medio.
c) La información referente a los datos personales contará además de las medidas de nivel básico y medio, con las calificadas de nivel alto.

VIGÉSIMO TERCERO: Los archivos temporales que contengan información confidencial serán borrados una vez que hayan dejado de ser necesarios para los fines que motivaron su creación.

VIGÉSIMO CUARTO: La información confidencial y reservada que se encuentre en documentos físicos se mantendrá en lugares protegidos contra las inclemencias del clima, procurando que se encuentren bajo llave y contenidos dentro de archiveros, de manera que se evite su alteración, pérdida o acceso no autorizado.

VIGÉSIMO QUINTO: Se designarán contraseñas personalizadas a los responsables y encargados de información confidencial contenida en medios automatizados; entendiéndose éstos, como el 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.

VIGÉSIMO SEXTO: Para el resguardo de los datos personales automatizados se tomarán las siguientes medidas:

a) Asignar un espacio seguro y adecuado.
b) Controlar el acceso físico a las instalaciones.
c) Contar con lugares que cumplan con las condiciones de seguridad.
d) Realizar procedimiento de control de asignación y renovación de claves de acceso a los sistemas.
e) Realizar procedimientos de control, registro de asignación y baja de equipos de cómputo de los servidores públicos que manejen información protegida, considerando las siguientes actividades:
    I. En caso de ser asignación, se debe configurar con las medidas de seguridad necesarias, tanto a nivel operativo como de infraestructura.
    II. Verificar y llevar un registro del contenido del equipo para facilitar los reportes del usuario que lo reciba o que lo entregue.
f) Implantar procedimientos de control y medidas de seguridad.

VIGÉSIMO SÉPTIMO: De conformidad al Lineamiento Cuadragésimo Primero de los Lineamientos Generales para la Protección de Información Confidencial y Reservada, se seguirán los siguientes criterios:

I. Nivel básico.

a) Se elaborará e implementará un documento que contenga las medidas de seguridad previstas para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información. Dicho documento contendrá los siguientes aspectos:

1. Ámbito de aplicación del documento con especificación detallada de los datos protegidos.
2. Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido.
3. Funciones y obligaciones del responsable.
4. Estructura y descripción de los sistemas de información.
5. Los procedimientos de realización de copias de respaldo y de recuperación de los datos.

b) Se tendrá un registro de las personas que tengan acceso autorizado a los Sistemas de Información Confidencial y Reservada, para lo cual se establecerá un proceso de identificación y autentificación para dicho acceso.

c) Exclusivamente el personal autorizado en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado previamente a los datos y recursos, conforme a los criterios establecidos por el responsable del fichero.

d) Los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado para ello en el documento de seguridad.

La transferencia de soportes informáticos que contengan datos de carácter personal, únicamente podrá ser autorizada por el responsable de los mismos.

II. Nivel medio.

a) Se creará un documento de seguridad que deberá contener, además de lo dispuesto en el inciso a) de la fracción que antecede, la identificación del responsable o responsables de seguridad, los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento y las medidas que sea necesario adoptar cuando un soporte y/o sistema vaya a ser desechado o reutilizado.

b) El responsable de la información confidencial y reservada podrá designar uno o varios responsables de seguridad, encargados de coordinar y controlar las medidas definidas en el documento de seguridad, sin que esto suponga una delegación del compromiso que corresponde al Responsable.

c) Para verificar que se estén aplicando correctamente las medidas de seguridad, la Dirección de Protección de Datos Personales, realizará auditorías periódicas a los sistemas de información e instalaciones de tratamiento de datos, al menos cada dos años.

El informe de auditoría deberá dictaminar sobre la adecuación de las medidas de seguridad correspondientes a este nivel, debe contener la identificación de las deficiencias y proponer las medidas correctoras o complementarias necesarias.

Además deberá incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

d) El responsable de la información que contenga datos personales debe establecer un mecanismo que permita la identificación, de forma inequívoca y personalizada, de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado, además de limitar la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

e) Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se encuentren ubicados los sistemas de información con datos de carácter personal.

f) Deberá establecerse un sistema de registro de entrada de soportes informáticos que permita, directa o indirectamente, conocer:

1. El tipo de soporte.
2. La fecha, hora y el emisor.
3. El número de soportes y el tipo de información que contienen.
4. En caso de transferencia la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

g) Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten con datos de carácter personal no se realizarán con datos reales, salvo que se compruebe el nivel de seguridad correspondiente al tipo de información tratada.

III. Nivel alto.

a) Se tomarán en cuenta las disposiciones emitidas para la aplicación de los niveles de seguridad básico y medio.

b) En caso de que sea necesaria la transferencia de sistemas electrónicos, la distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte.

c) De cada acceso se guardarán, como mínimo:

1. La identificación del usuario.
2. Fecha y hora en que se realizó
3. Documento accedido y el tipo de acceso (autorizado o denegado).

En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido, el período mínimo de conservación de los datos registrados será de dos años.

TRANSITORIOS

PRIMERO.- Los presentes criterios entrarán en vigor al día siguiente de su aprobación por el Consejo del Instituto de Transparencia e Información Pública de Jalisco.

SEGUNDO.- Los presentes criterios deberán ser publicados en la página web del Instituto.

Remítase al Instituto de Transparencia e Información Pública de Jalisco, para efecto de su autorización, en términos del artículo 30, punto 1, fracción II de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.

Cynthia Patricia Cantero Pacheco
Presidenta del Comité

María Guadalupe Plascencia Vázquez
Secretario del Comité

Jorge Alberto Contreras Bravo
Director Jurídico