CRITERIOS GENERALES EN MATERIA DE PROTECCIÓN DE INFORMACIÓN CONFIDENCIAL Y RESERVADA, QUE DEBERÁN OBSERVARSE EN EL INSTITUTO DE JUSTICIA ALTERNATIVA EN SU CARÁCTER DE SUJETO OBLIGADO EN LA LEY DE INFORMACIÓN PÚBLICA DEL ESTADO DE JALISCO.

El Pleno del Comité de Clasificación de Información Pública del Instituto de Justician Alternativa del Estado de Jalisco, con fundamento en lo dispuesto por los artículos 25 fracciones IX, XIV y XV, y 30 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, y

CONSIDERANDO:

I. Que de conformidad con el artículo 6° de la Constitución Política de los Estados Unidos Mexicanos, toda la información en posesión de las autoridades es publica , y solo puede ser reservada por razones de interés público, además que se debe proteger aquella que se refiere a la vida privada y los datos personales, con la respectiva obligación de proteger dicha información, mientras que en el precepto 16, que tiende a limitar la intromisión del Estado en el ámbito de la persona;

II. Que el derecho internacional protege el derecho humano de acceso a la información pública, pero a la par debe atender a la protección de la seguridad nacional, el orden público, la salud o moral, en términos del artículo 13 de la Convención Americana sobre Derechos Humanos y el Precepto 19 del Pacto Internacional de Derechos Civiles y Políticos;

III. Que el Instituto de Transparencia e Información Pública del Estado, tiene la facultad de emitir lineamientos en materia de protección de información confidencial y reservada y en base a estos, el Instituto de Justicia Alternativa del Estado a través de sus comité de clasificación emite los criterios generales en tal materia en los siguientes términos;

CRITERIOS GENERALES EN MATERIA DE PROTECCIÓN DE INFORMACIÓN CONFIDENCIAL Y RESERVADA, QUE DEBERÁN OBSERVARSE EN EL INSTITUTO DE JUSTICIA ALTERNATIVA DEL ESTADO DE JALISCO.

CAPÍTULO I
DISPOSICIONES GENERALES.

PRIMERO.- Los presentes criterios generales en materia de protección a la información confidencial y reservada, son de observancia general y vinculatoria para todas las unidades administrativas que conforman el Instituto de Justicia Alternativa y serán la base para establecer los procedimientos que deberán observar para el debido manejo, mantenimiento, seguridad y protección de la misma.

Lo anterior, sin perjuicio que en el ejercicio de sus atribuciones todo el personal del Instituto de Justicia Alternativa deberá apegarse estrictamente a los supuestos previstos por la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y su Reglamento, Los Lineamientos Generales para la Protección de la Información Confidencial y Reservada emitidos por el Instituto de Transparencia e Información Pública del Estado de Jalisco, el Reglamento de Transparencia y Acceso a Información Pública del Instituto de Justicia Alternativa del Estado y en su caso a otros ordenamientos que sean aplicables.

SEGUNDO.- Para los efectos de los presentes criterios se emplearan las siguientes definiciones:

I. Comité: El Comité de Clasificación de Información Pública del Instituto de Justicia Alternativa del Estado.
II. Consejo: El Consejo del Instituto de Transparencia e Información Pública del Estado de Jalisco.
III. ITEI: Instituto de Transparencia e Información Pública del Estado de Jalisco.
IV. IJA: Instituto de Justicia Alternativa del Estado de Jalisco.

V. Ley: Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.

VI. Reglamento: Reglamento de Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.

VII. Unidad: La Unidad de Transparencia del Instituto de Justicia Alternativa del Estado de Jalisco.

TERCERO.- El IJA a través de su Comité de Clasificación de Información Pública, elaborara sus políticas con relación a la protección de la información confidencial, de conformidad con los artículos 17 y 24 de la Ley, mismas que deberán dar a conocer a las personas físicas y o jurídicas cuando estas hagan entrega de información con dicho carácter.

CUARTO.- Para los efectos de los presentes criterios generales, se entenderá como “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 del IJA.

Los bienes protegidos para el caso de la información confidencial se identifican con el honor, la intimidad, cualquier otro que se dirija a la persona y específicamente:

Es Información Confidencial:

I. Los datos personales de una persona física identificada o identificable relativos a:
   a) Origen étnico o racial;
   b) Características físicas, morales o emocionales;
   c) Vida afectiva o familiar;
   d) Domicilio;
   e) Número telefónico y correo electrónico;
   f) Patrimonio;

g) Ideología, opinión política y creencia o convicción religiosa y filosófica;
h) Estado de salud física y mental e historial médico,
i) Preferencia sexual, y
j) Otras análogas que afecten su intimidad;

II. La entregada con tal carácter por los particulares, siempre que:
a) Se precisen los medios en que se contiene; y
b) No se lesione derechos de terceros o se contravengan disposiciones de orden público;

III. La considerada como confidencial por disposición legal expresa.

Es información reservada:

I. Aquella información pública, cuya difusión:

a) Comprometa la seguridad del estado, del municipio o la seguridad pública;

b) Dañe la estabilidad financiera o económica del Estado;

c) Ponga en Riesgo la vida, seguridad o salud de cualquier persona;

d) Cause perjuicio grave a las actividades de verificación, inspección y auditorias, relativas al cumplimiento de las leyes y reglamentos;

e) Cause perjuicio grave a la recaudación de las contribuciones;

f) Cause perjuicio grave a las actividades de prevención y persecución de los delitos, o de impartición de la justicia; o

g) Cause perjuicio grave a las estrategias procesales en procesos judiciales o procesos judiciales o procedimientos administrativos cuyas resoluciones no hayan causado estado;

II. Las averiguaciones previas;

III. Los Expedientes judiciales en tanto no causen estado;

IV. Los expedientes de los procedimientos administrativos seguidos en forma de juicio en tanto no causen estado;

V. Los Procedimientos de responsabilidad de los servidores públicos, en tanto no se dicte la resolución administrativa o la jurisdiccional definitiva;

VI. La que contenga opiniones, recomendaciones o puntos de vista que formen parte del proceso deliberativo de los servidores públicos, en tanto no se adopte la decisión definitiva;

VII. La entregada con carácter de reservada o confidencial por autoridades federales o de otros estados, o por organismos internacionales;

VIII. La considerada como secreto comercial, industrial, fiscal, bancario, fiduciario, bursátil o cualquier otro, por disposición legal expresa;

IX. Las bases de datos, pregunta o reactivos para la aplicación de exámenes de admisión académica, evaluación psicológica, concursos de oposición o equivalentes; y

X. La considerada como reservada por disposición legal expresa.

QUINTO.- Los servidores públicos del IJA 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 sucederá con las personas que sean contratadas por el IJA bajo cualquier otro régimen.

CAPITULO II
PROTECCION DE LA INFORMACION
CONFIDENCIAL Y RESERVADA
Sección I
De la Información Reservada

SEXTO.- Para dictaminar si la información tiene el carácter de reservada. El Comité de Clasificación de la Información Pública del IJA deberá apegarse a la regulación de la Ley, los Reglamentos y Lineamientos y, acreditar mediante la

prueba de daño que se actualizan los supuestos señalados, y cuyo resultado se asentara en un acta.

SEPTIMO.- En el caso de la información reservada, únicamente deberá ser manejada por el personal del IJA directamente involucrado en las labores propias de la generación y manejo de la información.

OCTAVO.- La información reservada deberá encontrarse resguardada, en lugar seguro, de modo que no se conserve en archivos de fácil acceso al público.

NOVENO.- El ITEI, podrá tener acceso en todo momento a la información reservada, así como a la inspección y vigilancia de los esquemas de mantenimiento o aseguramiento que fije el IJA mediante los criterios generales que determine.

Sección II

De la Información Confidencial

DECIMO.- A efecto de determinar si la información que posea el IJA, es información confidencial, deberán considerarse las siguientes hipótesis.

I. Que la misma sea concerniente a una persona física, identificada o 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 previa a la vida íntima y familiar, y

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

DECIMO PRIMERO.- 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.

DECIMO SEGUNDO.- Cuando el IJA reciba información que tenga el carácter de confidencial, este deberá hacer del conocimiento de la persona física o jurídica que entregue dicha información, lo siguiente:

I. Las disposiciones que sobre dicha información prevé la Ley:
II. Las disposiciones contenidas en los Lineamientos y en los demás que sobre el particular emita el Consejo del ITEI.
III. Que se obliga a conducirse con verdad respecto a la información confidencial que entregue, de acuerdo a lo previsto por los ordenamientos legales señalados en las fracciones que anteceden.

DÉCIMO TERCERO.- 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 aun 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.

DECIMO CUARTO.- En el tratamiento particularmente de los datos personales, el IJA deberá 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.

DECIMO QUINTO.- Por principio de licitud se entenderá toda aquella recolección de datos personales que se realice a través de las medidas legales o reglamentarias del IJA previsto para tales efectos.

DECIMO SEXTO.- 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.

DECIMO SEPTIMO.- El principio de consentimiento, se refiere a la manifestación de voluntad libre, inequívoca, especifica e informada, mediante la cual el interesado consiente el tratamiento de sus datos personales.
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.

DECIMO OCTAVO.- 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 trataran dichos datos.

DECIMO NOVENO.- 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 IJA posea.

VIGESIMO.- A efecto de cumplir con el principio de calidad a que se refiere el criterio 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 del IJA 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.

VIGESIMO PRIMERO.- El principio de finalidad, consiste en que los datos personales recabados por IJA deberán ser tratados exclusivamente para la finalidad que fueron obtenidos.

VIGESIMO SEGUNDO.- 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.

VIGESIMO TERCERO.- 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.

VIGESIMO CUARTO.- 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 Ia protección de Ia Información Confidencial.

VIGESIMO QUINTO.- Los datos personales deberán ingresarse en un sistema de información confidencial previamente diseñado conforme a Ia 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 Ia información confidencial previstos por Ia Ley.

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

VIGESIMO SÉPTIMO.- Las medidas de seguridad que implemente el IJA deberán ser suficientes para garantizar la integridad, confiabilidad, secrecía y disponibilidad de la información confidencial mediante acciones que eviten su alteración perdida, transmisión y acceso no autorizado, de conformidad a la Ley, a los Lineamientos y a los demás que emita el Consejo del ITEI.

VIGESIMO OCTAVO.- El IJA podrá implementar otras medidas adicionales que según su normatividad, organización y operatividad se adecuen, siempre con la finalidad de proteger la información confidencial.

CAPITULO lll
DISPOSICIONES COMUNES PARA LA SEGURIDAD DE LA INFORMACION CONFIDENCIAL Y RESERVADA

VIGESIMO NOVENO.- Las medidas de seguridad que implementen IJA, serán las suficientes para garantizar Ia integridad, confiabilidad, confidencialidad y disponibilidad de Ia información protegida mediante acciones que eviten Ia alteración, perdida, trasmisión y acceso no autorizado, de conformidad a Ia Ley, su Reglamento y los presentes criterios.

TRIGÉSIMO.- Son tipos de seguridad:

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

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

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

IV. De cifrado: Consiste en Ia implementación de algoritmos, claves, contraseñas, así como dispositivos concretos de protección que garanticen Ia integralidad y confidencialidad de Ia 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.

TRIGÉSIMO 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) Capias de respaldo y recuperación.

II. Media.- Se refiere a Ia adopción de medidas de seguridad cuya aplicación corresponde a aquellos sistemas relativos a Ia 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 Ia 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 media, 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 IJA adoptara 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 comunicara al Instituto, para su registro, el nivel de seguridad aplicable.

TRIGÉSIMO SEGUNDO.- 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 caratula 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 utilizaran mecanismos que aseguren que Ia información únicamente será tratada por el destinatario autorizado a recibirla.

d) Comunicar a los destinatarios sobre Ia responsabilidad que estos adquieren al recibir Ia información a que se refiere este artículo.

e) Contenerse en sobre cerrado y sellado, cuyo traslado será a cargo de servidores públicos del IJA autorizado para ello.

f) Las demás medidas de protección que, de acuerdo a los riesgos y amenazas, el IJA considere necesario adoptar.

TRIGÉSIMO TERCERO.- Los responsables de recibir Ia información confidencial y/o reservada que se transfiere, estarán obligados a:

1) Firmar el acuse de recibo correspondiente, hacienda constar hora y fecha de recepción, así como Ia integridad del sobre recibido, registrando al efecto, que no existan indicios de violación o cualquier otra irregularidad.

2) Mantener resguardada Ia 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 Ia información recibida.

4) Realizar las acciones necesarias para contener Ia circulación de dicha información.

TRIGÉSIMO CUARTO.- Para la protección de la información confidencial, el IJA por conducto de su Director General, podrá adoptar, dependiendo del material de soporte en que se encuentre la información, las siguientes medidas administrativas, físicas y técnicas de seguridad:

I. Dar a conocer los presentes criterios generales, así como la normatividad relativa al manejo, mantenimiento, seguridad y protección de la información confidencial, la personal del IJA.

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 la 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 consideren aplicables, sin que se utilicen datos reales.

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.

TRIGÉSIMO QUINTO.- Los sujetos obligados podrán expedir un documento, de seguridad; el que contemplara las medidas administrativas, físicas y técnicas de seguridad aplicables a Ia información confidencial, particularmente a los datos personales, según las necesidades de cada soporte o material en el que se encuentre Ia misma.

El documento mencionado en el criterio 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 criterios, 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.

Capitulo IV
De los Responsables

TRIGÉSIMO SEXTO.- Para el cumplimiento de los presentes criterios 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 dé.

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

TRIGÉSIMO SÉPTIMO.- Para dar cumplimiento a lo dispuesto por el articulo 35 punto 1, fracción XI de Ia Ley, el IJA deberá contar con un Sistema de Información Reservada y un Sistema de Información Confidencial.

TRIGÉSIMO OCTAVO.- El IJA deberá registrar e informar al ITEI, según corresponda, lo establecido en el Capítulo Segundo, Sección Segunda de Ia Ley; para lo cual el Instituto desarrollara una aplicación que permita mantener actualizado el listado de sistemas que el IJA maneje.

TRIGÉSIMO NOVENO.- El IJA deberá inscribirlos en el Registro habilitado por el Instituto, en un plazo no mayor a los 10 días hábiles siguientes a Ia creación del mismo.

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

CUADRAGÉSIMO.- En el acuerdo de creación de los Sistemas de Información Reservada, El IJA deberá tomar en consideración los datos que se enlistan a continuación:

I. EL acta de clasificación sobre Ia cual se pueda identificar el rubro temático de Ia información reservada que se trate.

II. Unidad administrativa que genera, obtuvo, adquirió, o conserva Ia información.

Ill. Fecha de clasificación que se refiere al día, mes y ano, en el cual fue aprobada el acta de clasificación.

IV. La fundamentación legal sobre Ia cual se pretende sustentar el acto de clasificar Ia información como reservada.

V. El lapso de tiempo sobre el cual se reservara Ia información, especificando por evento o por Ia denominación de documento.

VI. En su caso, las partes del documento que se consideran como reservadas.

CUADRAGÉSIMO PRIMERO.- 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 Ia información

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

Ill. El origen de Ia Información Confidencial, así como el grupo de interesados al que va dirigido, es decir Ia procedencia o mecanismo por el que se obtienen Ia Información Confidencial o Ia Reservada (propio interesado, representante, ente público, etcétera), así como Ia indicación de Ia denominación del grupo o sector del que se realice Ia 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 podría legislación aplicable a la materia entendiendo por cesión, toda obtención de datos resultante de la consulta de un archive, registro, base o banco de datos, una publicación de los datos contenidos en el 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, media o alto.

CUADRAGÉSIMO TERCERO.- 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 Criterios entraran en vigor al día siguiente de su aprobación por parte del Consejo del Instituto de Transparencia e Información Pública del Estado de Jalisco.

Así lo acordó el Comité de Clasificación de Información Pública del Instituto de Justicia Alternativa del Estado de Jalisco, en la Primera Sesión Extraordinaria del día 15 de Octubre del 2014.

Presidente del Comité de Clasificación de Información Pública y Secretario Técnico en Funciones Director General del Instituto de Justicia Alternativa del Estado de Jalisco actuando de conformidad con el régimen de suplencias contemplado los artículos 33 fracción III de la Ley de Justicia Alternativa del Estado, así como en la fracción XVII del artículo 35 del Reglamento Interno del mismo Instituto.

LIC. I. ALFONSO REJÓN CERVANTES

CONTRALOR DEL INSTITUTO DE JUSTICIA ALTERNATIVA DEL ESTADO DE JALISCO

LIC. GUILLERMO AMEZQUITA GUTIÉRREZ

SECRETARIO TÉCNICO DEL COMITÉ DE CLASIFICACIÓN DE INFORMACIÓN PÚBLICA Y COORDINADOR DE LA UNIDAD DE TRANSPARENCIA E INFORMACIÓN DEL INSTITUTO DE JUSTICIA ALTERNATIVA DEL ESTADO DE JALISCO

ROBERTO ARMANDO CRUZ BRAVO