LINEAMIENTOS GENERALES PARA EL MANEJO DE INFORMACIÓN RESTRINGIDA Y LA PROTECCIÓN DE LOS DATOS PERSONALES EN POSESIÓN DE LOS SUJETOS OBLIGADOS DEL ESTADO DE SONORA.

CAPÍTULO I
Disposiciones Generales

Sección Primera
De la clasificación

Artículo 1- Los presentes lineamientos son imperativos y de observancia general para los sujetos obligados y se expiden de conformidad con lo dispuesto por los artículos 7 y 33 de la Ley de Acceso a la Información Pública para el Estado de Sonora; tienen por objeto establecer los criterios con base en los cuales los titulares de las unidades administrativas de los sujetos obligados, clasificarán la información que posean, la desclasificarán y modificaran, en su caso, además de prever las políticas generales, condiciones y requisitos mínimos para el debido manejo y custodia de sus sistemas de datos, así como los procedimientos y/o medidas de seguridad que deberán observar los sujetos obligados para garantizar a los particulares la facultad de decisión sobre el uso y destino de sus datos personales de conformidad con los principios establecidos en la Ley, con el propósito de asegurar su adecuado tratamiento e impedir su transmisión ilícita y lesiva para la dignidad y derechos del afectado.

Artículo 2.- Para los efectos de los presentes lineamientos se emplearán las definiciones contenidas en los artículos 3 de la Ley de Acceso a la Información Pública del Estado y las que se contengan en las disposiciones generales que emita el Instituto, además de las siguientes:

I. Sistema de Datos Personales: Constituye el conjunto ordenado de datos personales que estén en posesión de los sujetos obligados, con independencia de su forma de acceso, creación, almacenamiento u organización;

II. Tratamiento: Conjunto de operaciones y procedimientos físicos o automatizados que permitan recabar, registrar, reproducir, conservar, organizar, modificar, transmitir y cancelar datos personales,

III. Disociación de datos: Consiste en todo tratamiento o procedimiento que impida que los datos personales puedan asociarse al titular de éstos, o permitir por su estructura, contenido o grado de desagregación, la identificación individual del mismo;

IV. Destinatario: Cualquier persona física o moral pública o privada que recibe datos personales;

V. Responsable: El servidor público titular de la unidad administrativa designado por el titular del sujeto obligado, que decide sobre el tratamiento físico o automatizado de

datos personales, así como el contenido y finalidad de los sistemas de datos personales;

VI. Encargado: El servidor público o cualquier otra persona física o moral facultado por un instrumento jurídico o autorizado legalmente por el Responsable para llevar a cabo el tratamiento físico o automatizado de los datos personales;

VII. Titular de los datos: Persona física a quien se refieren los datos personales que sean objeto de tratamiento;

VIII. Transmisión: Toda entrega total o parcial de datos personales realizada por las dependencias y entidades a cualquier persona distinta al titular de los datos, mediante el uso de medios físicos o electrónicos tales como la interconexión de computadoras, interconexión de bases de datos, acceso a redes de telecomunicación, así como a través de la utilización de cualquier otra tecnología que lo permita;

IX. Transmisor: Dependencia o entidad que posee los datos personales objeto de la transmisión; y,

X. Usuario: Servidor público facultado por la normatividad 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.

Artículo 3.- De acuerdo a lo establecido por el artículo 4 de la Ley, en la interpretación de la misma y de los presentes lineamientos deberán favorecerse los principios de legalidad, certeza jurídica, imparcialidad, información, celeridad, veracidad y máxima publicidad de la información en posesión de los sujetos obligados y transparencia en los documentos que registren sus actos, salvo las excepciones respecto a la información restringida en sus modalidades de reservada y confidencial, así como el derecho fundamental que comprende la protección de la vida privada y los datos personales contempladas en la Ley y en los presentes lineamientos.

Artículo 4.- Los titulares de las unidades administrativas de los sujetos obligados que cuenten, cuando menos, con nivel de director general o su equivalente con nivel directivo respecto a la estructura orgánica que corresponda, serán los responsables de clasificar la información a su cargo de conformidad con la Ley, así como los presentes lineamientos. Sin perjuicio de lo anterior, y con la finalidad de brindar apoyo técnico y jurídico a dichos titulares, cada sujeto obligado podrá establecer la conformación de un Comité de Información al que invariablemente pertenecerá el titular de la dependencia o entidad pública o el servidor público que, para tal efecto, él mismo designe, quien lo presidirá.

Tratándose de sujetos obligados que cuenten con sistemas de datos personales, deberán contar con el antes mencionado comité de información.

Articulo 4 bis.- Los comités de información además de adoptar sus decisiones por mayoría de votos, contarán con las siguientes funciones:

I. Supervisar la aplicación de los criterios de clasificación de la información reservada y confidencial, expedidos por el Instituto;

II. Actualizar, inspeccionar, establecer y aprobar, en su caso, los procedimientos, mecanismos, herramientas, medidas de seguridad y responsabilidades a seguir por parte de los servidores públicos que tengan bajo su custodia o manejo el sistema de datos personales del sujeto obligado correspondiente;

III. Revisar la clasificación de información y resguardarla conforme a los criterios y lineamientos que al efecto expida el Instituto, elaborando, en los casos precedentes, la versión pública de dicha información;

IV. Elaborar, aprobar y supervisar la actualización de los índices de información reservada, mismos que se deberán remitir al Instituto, por conducto de la unidad de enlace, durante los primeros veinte días de los meses de enero y julio de cada año. Lo anterior con fundamento en el artículo 26 de la Ley de Acceso a la Información Pública del Estado de Sonora;

V. Establecer, de conformidad con las disposiciones reglamentarias en la materia, las medidas que coadyuven a una mayor eficiencia en la atención de las solicitudes de acceso a la información y protección de datos personales; y,

VI. Coordinar y supervisar las acciones realizadas en su respectivo órgano de gobierno para el cumplimiento de las disposiciones previstas en la Ley y en los presentes lineamientos.

Artículo 5.- La clasificación de la información reservada tiene por fin imponer una restricción temporal para permitir el acceso a dicha información, siendo requisito indispensable para su clasificación la existencia del acuerdo fundado y motivado, en cada caso, que sirva de base para dicha clasificación.

La información confidencial tiene como fin imponer una restricción permanente para permitir el acceso a dicha información; su clasificación será por estricto derecho.

Artículo 6.- Para clasificar la información como reservada, los titulares de las unidades administrativas y/o, en su caso el comité de información deberán atender a lo dispuesto por el Capítulo II del Título Segundo de la ley, así como a los presentes lineamientos.

La clasificación de la información podrá llevarse a cabo sobre la totalidad de un expediente o sólo respecto de alguno o algunos de los documentos que integren el mismo, así como de otros documentos en lo individual aunque no formen parte de un expediente; se podrán incluso clasificar como reservados un conjunto de expedientes o archivos.

Artículo 7.- En el caso de información reservada, deberá establecerse el período de reserva, el que podrá ser por diez años prorrogables con anterioridad a su conclusión, en caso de subsistir las causas que originaron su clasificación o aparezcan otras de igual o mayor gravedad; así mismo el período de reserva puede ser menor a diez años atento a la previsibilidad de la extinción de las causales que le dieron origen. La información confidencial permanecerá como tal por tiempo indefinido, salvo lo dispuesto en el artículo 36 de los presentes lineamientos y la legislación aplicable.

El período de reserva correrá a partir de la fecha en que se clasifica el archivo, expediente o documento.

Artículo 8.- Los titulares de las unidades administrativas y/o, en su caso el comité de información correspondiente, al momento de responder a alguna solicitud de información en su caso, fundarán y motivarán la negación de la información sólo en los casos en que hubiese acuerdo de información reservada, siendo público el mismo cuando para tales efectos se requiera, mediante solicitud de acceso de conformidad con la Ley o normatividad aplicable.

Artículo 9.- En los expedientes y documentos que contengan partes o secciones reservadas o confidenciales, los titulares de las unidades administrativas y/o, en su caso el comité de información deberán señalar aquellas que para su publicidad deban omitirse a efecto de identificarlas. Asimismo, deberán reproducir la versión pública de los expedientes o documentos en caso de recibir una solicitud respecto de los mismos, sin perjuicio de que la dependencia o entidad determine elaborar versiones públicas en cualquier momento, o bien, al organizar sus archivos.

Para emitir versiones públicas de los documentos o expedientes que contengan información reservada o confidencial será necesario testar o eliminar la parte de la información que actualice los supuestos legales para la restricción.

Artículo 10.- Al clasificar la información no será suficiente que el contenido de la misma esté directamente relacionado con las materias que se protegen en dicho artículo, sino que deberá también considerarse la existencia de elementos objetivos que permitan determinar si la difusión de la información causaría un daño presente, probable y específico a los intereses jurídicos tutelados.

Por fundamentación se entiende además de las expresiones antes citadas, el señalar, expresar o invocar los preceptos jurídicos contenidos en la Ley o en alguna otra disposición jurídica, en los que se prevea que cierta información cumple con las características para ser clasificada como reservada, debiendo señalarse específicamente los ordenamientos jurídicos, artículo, párrafo, fracción o inciso que expresamente le otorgan ese carácter.

Así mismo, cuando la información se clasifique en los términos precitados los titulares de las unidades administrativas además de la fundamentación como antes se expuso, deberán motivar la clasificación.

Por motivación se entiende los argumentos, razonamientos o expresiones en base a las cuales se justifique que cierta información encuadra en la hipótesis de una disposición jurídica conforme a la cual dicha información debe ser clasificada como reservada.

Artículo 11.- Los titulares de las unidades administrativas de los sujetos obligados y/o, en su caso el comité de información llevarán a cabo la clasificación de la información en el momento en que:

I.- Se genere, administre, obtenga, adquiera, transforme, posea o conserve la información;

II.- Se reciba la información; o

III.- Se reciba la solicitud de acceso a la información, en caso de documentos que no se hubieren clasificado previamente.

Artículo 12.- Los titulares de las unidades administrativas y/o, en su caso el comité de información deberán tener conocimiento y llevar un registro de los servidores públicos que por la naturaleza de sus atribuciones, tengan acceso a los expedientes y documentos clasificados como reservados o confidenciales. Asimismo, deberán asegurarse de que dichos servidores públicos tengan conocimiento de la responsabilidad en el manejo de información restringida, misma que perdurará aún después de finalizada la relación laboral entre el sujeto obligado y los responsables, encargados o usuarios del sistema de información.

Artículo 13.- Excepcionalmente en ausencia de los titulares de las unidades administrativas, la información será clasificada por el servidor público que los supla, en los términos del Reglamento Interior o Estatuto Orgánico que corresponda a dicho sujeto obligado.

Artículo 14.- En el intercambio de información entre sujetos obligados para el ejercicio de sus atribuciones, los documentos deberán señalar la clasificación, en su caso, con los requisitos que exige el artículo 24 de la ley y los presentes lineamientos.

Sección Segunda
De la desclasificación

Artículo 15.- Los expedientes y documentos clasificados como reservados podrán desclasificarse cuando:

I.- Haya transcurrido el período de reserva que indique la ley;

II.- No habiendo transcurrido el período de reserva, cuando ya no subsistan las causas que dieron origen a la clasificación, atendiendo las circunstancias de modo, tiempo y lugar; para este supuesto únicamente se exige acuerdo fundado y motivado; o

III. Lo ordene el Instituto de Transparencia Informativa del Estado de Sonora y para los fines a que se refiere la ley en los artículos 20, 25 y demás relativos.

Excepcionalmente, los sujetos obligados podrán ampliar el período de reserva hasta por un plazo adicional de diez años, siempre y cuando subsistan las causas que dieron origen a su clasificación o aparezcan otras de igual o mayor gravedad, así como también, en tal caso, la citada ampliación se formule tres meses antes de que concluya el plazo original de reserva.

La restricción al acceso de la información concluye de pleno derecho por el solo transcurso del tiempo, sin necesidad de resolución o acto administrativo alguno.

Artículo 16.- La desclasificación puede llevarse a cabo por:

I. El titular de la unidad administrativa y/o el comité de información al cual está integrado éste;

II. El Instituto de Transparencia Informativa del Estado de Sonora; y

III.- El solo transcurso del tiempo por el que originalmente fue clasificada, salvo que se amplíe el período.

Artículo 17.- La desclasificación de la información requiere la modificación del índice en el que se señaló la información como clasificada, indicando la fecha y motivo de desclasificación; además, procede como consecuencia necesaria la invalidación de los acuerdos respectivos, así como los formatos y portadas que hubiesen identificado a la misma como restringida, sin perjuicio de que dicha información deba ser clasificada posteriormente por circunstancias supervenientes.

CAPÍTULO II
De la información reservada

Artículo 18.- Se clasificará como reservada la información cuando se comprometa la seguridad nacional, del Estado o los municipios, esto es, que con la difusión de la información:

I.- Se ponga en riesgo acciones destinadas a proteger la integridad, estabilidad y permanencia de la Nación, así como la defensa exterior y la seguridad interior de la Federación, orientadas al bienestar general de la sociedad que permitan el cumplimiento de los fines del Estado Constitucional;

II.- Se pueda causar perjuicio o daño irreparable a las funciones públicas, comprometa la integridad, la estabilidad, la permanencia, la gobernabilidad democrática o la seguridad del Estado de Sonora y sus municipios, así como aquélla que pudiere poner en peligro la propiedad o posesión del patrimonio estatal o municipal;

III.- Se ponga en riesgo las acciones destinadas a proteger la estabilidad de las instituciones del Estado de Sonora y sus municipios, cuando la difusión de la información pueda afectar la integridad física de las máximas autoridades de los tres poderes del Estado y de sus órganos; y

IV.- Se ponga en riesgo acciones destinadas a proteger la integridad, estabilidad y permanencia del Estado de Sonora y sus municipios, la gobernabilidad democrática y la seguridad de sus habitantes, orientadas al bienestar general de la sociedad que permitan el cumplimiento de los fines del Estado Constitucional.

En ese orden de ideas, deberá entenderse que:

1.- Se ponen en riesgo las acciones destinadas a proteger la integridad, estabilidad y permanencia de la Nación, así como la defensa exterior y la seguridad interior del Estado Mexicano cuando la difusión de la información pueda:

a) Menoscabar o lesionar la capacidad de defensa del territorio nacional, entendiendo como tal el establecido en el artículo 42 de la Constitución Política de los Estados Unidos Mexicanos, por otros estados o sujetos de derecho internacional, o

b) Quebrantar la unidad de las partes integrantes de la Federación señaladas en el artículo 43 de la Constitución Política de los Estados Unidos Mexicanos.

2.- Se ponen en riesgo las acciones destinadas a proteger la estabilidad de las instituciones de la Federación, Estado y municipios cuando la difusión de la información pueda afectar la integridad física de las máximas autoridades de los tres poderes del Estado y de sus órganos.

3.- Se ponen en riesgo las acciones destinadas a proteger la gobernabilidad democrática cuando con la difusión de la información se pueda:

a) Impedir el derecho a votar y a ser votado; o

b) Obstaculizar la celebración de elecciones.

4.- Se ponen en riesgo las acciones destinadas a proteger la seguridad del Estado o de los municipios cuando la difusión de la información pueda:

a) Obstaculizar o bloquear operaciones contra la delincuencia organizada, ya sea: toda aquella información que constituya estrategias preventivas para mantener el orden social; acciones, operativos y programas para la vigilancia, así como aquella que integre operativos para la seguridad y custodia de personas y, aquellas acciones que por sus propias características, su divulgación ponga en riesgo su realización, por su especulación o interpretación errónea.

b) Obstaculizar o bloquear actividades de planeación estratégica de seguridad.

c) Menoscabar o dificultar las estrategias para combatir la comisión de los delitos contra la seguridad del Estado, previstos en el Título Octavo del Código Penal de esta Entidad Federativa.

d) Destruir o inhabilitar la infraestructura de carácter indispensable para la provisión de bienes o servicios públicos de agua potable, vías generales de comunicación o servicios de emergencia, o

e) Menoscabar o lesionar la capacidad de defensa del territorio del Estado, poniendo en riesgo o vulnerabilidad la integridad de las fuerzas armadas de la federación, de las policías federales, estatales y municipales; así como atentar en contra de la soberanía e independencia de la Nación, de los Estados, de los municipios o de las partes integrantes de su territorio; que pongan en riesgo o vulneren la estructura física de los edificios públicos, vías de comunicación, la integridad de los servidores públicos, los sistemas de información o cualquier otra circunstancia que atente contra la continuidad de las instituciones públicas y sean necesarias para salvaguardar el orden y la paz social.

5.- Se pone en peligro el orden público cuando la difusión de la información pueda:

a) Entorpecer los sistemas de coordinación interinstitucional en materia de seguridad pública.

b) Estropear o dificultar las estrategias contra la evasión de reos.

c) Quebrantar o limitar la capacidad de las autoridades para evitar la comisión de delitos, mediante el conocimiento del estado de fuerza de las instituciones, tales como; ubicación precisa de elementos de las distintas corporaciones policiales y de seguridad, equipamiento, armamento, vehículos, planos y proyectos de construcción de los inmuebles e instalaciones donde se encuentren las oficinas policiales y de seguridad, programas informáticos y los códigos utilizados en sistemas de radiocomunicación, o

d) Menoscabar o limitar la capacidad de las autoridades encaminadas a disuadir o prevenir disturbios sociales que pudieran desembocar en bloqueo de vías generales de comunicación o manifestaciones violentas.

Artículo 19.- La información se clasificará como reservada cuando, con su difusión, se afecte la conducción de las negociaciones de acuerdos interinstitucionales y pueda poner en peligro las acciones encaminadas a la consecución de acuerdos del Estado o los municipios con algún otro sujeto de carácter nacional o internacional; así como cuando exista información que por su contenido o naturaleza, de ser difundida pueda afectar el resultado de negociaciones entre Federación, Estados y municipios, como en el caso de acuerdos de coordinación, de inversión, de crédito o financiamiento, de seguridad pública, de desarrollo económico, de apoyos extraordinarios u otros semejantes, así como toda información que sea entregada al Estado o municipios con el carácter de reservada por cualquier persona pública o privada.

Asimismo, se menoscaban las relaciones internacionales cuando se difunda información entregada al Estado o los municipios con carácter de confidencial por otros estados, organismos internacionales o cualquier otro sujeto de Derecho Internacional Público y que por alguna razón se encuentre en los archivos de algunos de los sujetos obligados por la ley.

Artículo 20.- Se clasificará como reservada la información, cuando con su difusión se puedan lesionar los procesos de negociación y resultados de los diferentes órdenes de gobierno, en cumplimiento de su función pública y pueda ser perjudicial del interés público; se encuentran en el presente supuesto:

a) Los acuerdos con los diversos grupos sociales, cuya divulgación ponga en riesgo su celebración o culminación.

b) Procesos de licitación mientras no estén concluidos. En este caso lo serán las posturas, ofertas, propuestas o presupuestos generados con motivo de los concursos o licitaciones en proceso. Una vez adjudicados los contratos, la información dejará de ser reservada, y

c) Información relativa a propuestas, discusiones o proyectos de coordinación en cualquier materia, proyectos estratégicos de desarrollo, negociaciones fiscales, económicas, políticas, legales o financieras que en caso de darse a conocer puedan repercutir en el resultado de tales gestiones.

Artículo 21.- La información se clasificará como reservada cuando, con su difusión, se pueda dañar la estabilidad financiera o económica del Estado o de los municipios, siempre que su difusión limite la efectividad de proveer a la economía de dichos sujetos obligados de recursos en numerario o se pueda afectar severamente la estabilidad del sistema financiero en su conjunto y de los sistemas de pagos, en los términos de las disposiciones legales aplicables.

Así mismo se clasificará como reservada la información que pueda afectar el secreto comercial, industrial, fiscal, bancario, fiduciario, u otro considerado como tal por una disposición legal.

Artículo 22.- Cuando la difusión de la información pudiera poner en peligro la vida, la seguridad, la salud o el patrimonio de las personas, la misma se clasificará como reservada en los siguientes supuestos:

I.- La información que con su difusión se pueda menoscabar la capacidad de las autoridades de seguridad pública para preservar y resguardar la vida o la salud de las personas; enunciativamente se entienden para el presente supuesto los siguientes casos:

a) Revelación de nombres, adscripciones, asignaciones, bitácoras, roles de servicios, fotografías, cargos y funciones, en especial de los integrantes de los cuerpos policiales y de seguridad, o

b) Las estrategias para combatir las acciones delictivas distintas de la delincuencia organizada.

II.- Aquella que pudiera repercutir en alguna afectación a la integridad personal o familiar como en los casos de dar a conocer el patrimonio en su universalidad; y

III.- La información relacionada con la salud pública y el medio ambiente, cuya divulgación suponga un grave riesgo para la sociedad por obstaculizar o bloquear acciones tendientes a prevenir o combatir epidemias o enfermedades exóticas en el Estado.

El nombre de los servidores públicos es información de naturaleza pública. No obstante, y en referencia a lo establecido en el inciso a) fracción I del presente artículo, se podrán clasificar dichos nombres como información reservada, sólo cuando existan funciones operativas y/o de planeación a cargo de servidores públicos tendientes a garantizar de manera directa la seguridad pública del Estado y de los municipios, a través de acciones preventivas y correctivas encaminadas a combatir a la delincuencia en sus diferentes manifestaciones, poniendo en riesgo de anular, impedir u obstaculizar dichas acciones, mediante la publicidad de sus identidades.

Artículo 23.- Se clasificará como reservada la información que con su difusión, pueda causar perjuicio o afecte las actividades de verificación del cumplimiento de las leyes, así como la impartición de justicia, la prevención o persecución de los delitos y, de modo especial, las averiguaciones previas en trámite. Para este supuesto se considera reservada toda aquella información que pueda:

I.- Entorpecer o causar perjuicio a las actividades de verificación del cumplimiento de las leyes, toda aquella información relativa a los programas de visitas de inspección, supervisión, vigilancia o fiscalización que realizan las autoridades competentes para vigilar el cumplimiento de las diversas obligaciones establecidas en las disposiciones legales;

II.- Obstaculizar o bloquear la recaudación de contribuciones, tal es el caso de:

a) Información relativa a la hora, día, lugar, objeto, responsable de la diligencia de ejecución de resoluciones fiscales antes de llevarse a cabo, y

b) información que con su difusión pueda impedir u obstruir las actividades de captación, comprobación y fiscalización de ingresos tributarios realizados por las autoridades facultadas para ello, o de cualquier otra forma pueda afectar la recaudación de dichos ingresos.

III.- Estropear o dificultar las actividades de verificación del cumplimiento de las leyes, toda aquella información relativa a los programas de visitas de inspección o verificación que lleven a cabo las autoridades competentes, tales como órdenes de aprehensión, detenciones, volantas, retenes, cateos y cualesquier otra diligencia policial, ministerial o

judicial, comprendiendo además las de otras autoridades administrativas en materia de fiscalización, recaudación fiscal, verificaciones internas, revisiones administrativas a establecimientos, así como todos los actos relativos a las averiguaciones previas y las actuaciones en los procedimientos administrativos tramitados en forma de juicio por tribunales o instancias administrativas;

IV.- Menoscabar las actividades de prevención o persecución de los delitos, información relativa a los operativos que realizan las diversas corporaciones policiales y de seguridad; supuesto que se actualiza además cuando:

a) La difusión de la información pueda impedir u obstruir las acciones o medidas implementadas para evitar la comisión de los delitos.

b) Se difundan las atribuciones que ejerce el Ministerio Público durante la averiguación previa y las actuaciones ante los tribunales del Poder Judicial del Estado, y

c) Se difundan las acciones operativas y de vigilancia de las corporaciones policiales.

V.- Obstaculizar o bloquear la Impartición de justicia; como en el caso de:

a) La contenida en las diligencias de preparación del ejercicio de la Acción Penal. La información de las averiguaciones previas en trámite, es aquella que resulta de la etapa durante la cual el Ministerio Público realiza todas aquellas actuaciones y diligencias necesarias para conocer la verdad histórica de un hecho posiblemente constitutivo de delito, a efecto de ejercitar o no la acción penal.

b) La información a cargo de los tribunales para conocer y resolver respecto de los juicios, asuntos, diligencias y controversias conforme a los plazos, formas y procedimientos establecidos en las leyes.

c) La contenida en procesos administrativos de responsabilidad, antes de que sea resuelta la causa. Las resoluciones dictadas en los procesos administrativos de responsabilidad, una vez que hayan quedado firmes no serán reservadas ni confidenciales.

d) La contenida en los procedimientos que se encuentren en trámite en las distintas instancias, sino hasta concluida cada instancia.

e) La depositada en el secreto de los juzgados; y
f) La que contenga opiniones, recomendaciones o puntos de vista que formen parte del proceso deliberativo de los funcionarios judiciales, hasta en tanto no sea adoptada la decisión definitiva, la cual deberá estar documentada.

En ese sentido, la información que posean los sujetos obligados relacionada con las acciones y decisiones implementadas por los sujetos que intervienen en las diversas etapas de los procesos judiciales, administrativos o arbitrales, así como aquellos que se sustancian ante tribunales internacionales, se considerará reservada hasta en tanto

la resolución respectiva no haya causado estado o ejecutoria, salvo los casos en que se vulnere la protección del derecho a la intimidad de las personas o el interés público, en los términos de la ley y demás disposiciones aplicables.

Artículo 24.- Se excepcionarán de la reserva a que se refiere el lineamiento anterior:

I.- A aquellas personas que tengan debidamente acreditada su personalidad dentro del juicio, de conformidad con la normativa aplicable;

II.- Cuando se trate de juicios de responsabilidad administrativa en contra de algún funcionario o servidor público que sea parte y sea éste quién solicite la información acorde a los ordenamientos legales que rijan en cada caso; y

III.- Cuando se trate de juicios que por su naturaleza sea de interés público a juicio de los tribunales que conozcan del asunto.

Cuando existan procedimientos accesorios al juicio principal, las partes que integren éste último, podrán consultar en el expediente la información perteneciente a los primeros en todo momento de acuerdo con las leyes procesales aplicables.

Artículo 25.- Será reservada la información que, mediante su difusión pueda generar un impacto negativo, causar daños o perjuicios al interés general del Estado o de los municipios, tratándose de estudios, proyectos y presupuestos sobre el desarrollo estatal o municipal, en tanto no se inicie su ejecución o suponga un riesgo para su realización.

Artículo 26.- Se clasificará como reservada la información que con su difusión, se pueda lesionar o perjudicar los derechos derivados de propiedad intelectual, patentes o marcas en poder de los sujetos obligados; tal es el caso de la siguiente:

I.- La que debe mantenerse en reserva, por disposición de las leyes de la materia por tratarse de cuestiones industriales, comerciales, financieras, científicas, técnicas, de invenciones y patentes, que obren en poder del órgano de la administración pública de que se trate; y

II.- La de particulares recibida bajo promesa de reserva con motivo de la celebración de convenios, contratos o actos jurídicos para demostrar la funcionalidad o idoneidad sobre un producto o servicio, así como en los casos en que dicha información esté contenida en los bienes o insumos que se reciben de un proveedor.

Artículo 27.- Será reservada la información contenida en informes, consultas y toda clase de escritos y documentos relacionados con la definición de estrategias y medidas a tomar por los sujetos obligados, que aún cuando formalmente no sean objetos de prueba en un juicio o procedimiento en que intervengan éstos como parte, por relacionarse con tales diligencias, puedan afectar la actuación de la autoridad en materia de controversias legales.

Artículo 28.- Se considerará que la información puede generar una ventaja personal, ganancias o lucros indebidos en perjuicio de un tercero, propiciar una competencia desleal o constituir tráfico de influencias, y por lo tanto será reservada en los siguientes casos:

I.- Cuando en su liberación se contengan datos sobre los montos, cláusulas, pujas o datos de las personas que concursen o participen en licitaciones, contratos, convenios, concesiones, o subastas del Estado mientras estas no hayan concluido según el procedimiento autorizado para su realización;

II.- Cuando se trate de información correspondiente a documentos o comunicaciones internas que sean parte de un proceso deliberativo, previo a la toma de una decisión administrativa; y

III.- La que contenga las opiniones, recomendaciones o puntos de vista o que formen parte del proceso deliberativo de los servidores públicos, hasta en tanto no sea adoptada la decisión definitiva, la cual deberá estar documentada.

Se considerará que se ha adoptado la decisión administrativa cuando el o los servidores públicos responsables de tomar la última determinación resuelvan el proceso deliberativo de manera concluyente, sea o no susceptible de ejecución.

En el caso de procesos deliberativos cuya decisión sea impugnable, ésta se considerará adoptada de manera definitiva o firme, una vez que haya transcurrido el plazo respectivo sin que se haya presentado dicha impugnación.

También se considera que se ha tomado la decisión administrativa en un proceso deliberativo, cuando a juicio del responsable de tomar dicha decisión, se considere que aquél ha quedado sin materia o cuando por cualquier otra causa no se continúe con su desarrollo.

Artículo 29.- Se considerará información reservada por los sujetos obligados no oficiales, aquella cuya divulgación afecte sus estrategias o funcionamiento interno, así como aquella que expresamente se clasifique de esta manera por la autoridad previamente o en el acto de entregarla al propio sujeto obligado no oficial, sin perjuicio de que la autoridad pueda formular también esta clasificación con posterioridad, debiendo respetarla el sujeto obligado no oficial a partir de que reciba la notificación correspondiente.

CAPÍTULO III
De la información confidencial

Artículo 30.- Se considerará como información confidencial la siguiente:

I. La información que contenga datos personales de los particulares o los servidores públicos y, además, que esté relacionada con el derecho a la vida privada como:

a) La información patrimonial que los servidores públicos declaren en los términos de la ley de la materia, salvo que los declarantes autoricen su divulgación.

b) Los expedientes médicos de los servidores públicos y de los pacientes de hospitales públicos.

c) La de carácter personal contenida en los expedientes que integren la Defensoría de Oficio en materia penal, la Defensoría del Trabajo u otras similares en materia civil y familiar, así como la información de igual carácter contenida en los expedientes de las dependencias encargadas de la Seguridad Pública y del Poder Judicial, cuidando preponderantemente las materias familiar y en penal los delitos sexuales, en especial los detalles de los delitos que afecten el entorno intimo de las víctimas, la explotación de menores o integridad de las personas, o

d) La de carácter personal contenida en las actuaciones de la Comisión Estatal de los Derechos Humanos del Estado para la investigación de las denuncias y quejas por violaciones de derechos humanos. Serán accesibles a los particulares acorde a la normatividad vigente los procedimientos que realice cuando hayan concluido, las recomendaciones que, en su caso, emita el titular de ese organismo.

II.- La que sea entregada por los particulares a los sujetos obligados oficiales con reserva expresa de confidencialidad, cuando así lo permita la ley; y

III.- La que sea definida así por disposición expresa de una ley como en el caso de:

a) La información de carácter personal, que se obtenga legalmente al intervenir las comunicaciones privadas en los términos del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, o

b) La información proporcionada por las personas en el Censo de Población y Vivienda.

Artículo 31.- Serán datos de carácter personal, toda información sobre una persona, física o moral, identificada o identificable. Se considerará identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación, o en general, mediante uno o varios elementos específicos como son:

a) Origen étnico o racial;

b) Características físicas, incluyendo la información biométrica como el reconocimiento de iris, la huella dactilar, y otras análogas;

c) Características morales;

d) Características emocionales;

e) Vida afectiva;

f) Vida familiar;

g) Domicilio particular;

h) Números telefónicos particulares;

i) Patrimonio;

j) Ideología;

k) Opinión política;

l) Creencia o convicción religiosa;

m) Creencia o convicción filosófica;

n) Estado de salud física;

ñ) Estado de salud mental;

o) Claves informáticas, cibernéticas, códigos y correos electrónicos personales;

p) Número de seguridad social y Clave Única de Registro de Población;

q) Preferencia sexual; y

r) Otras análogas que afecten su intimidad, como la información genética.

Artículo 32.- La información confidencial que los particulares proporcionen a los sujetos obligados para fines estadísticos, que éstos obtengan de registros administrativos o aquéllos que contengan información relativa al estado civil de las personas, no podrán difundirse en forma nominativa o individualizada, o de cualquier otra forma que permita la identificación inmediata de los interesados, o conduzcan, por su estructura, contenido o grado de desagregación a la identificación individual de los mismos.

Artículo 33.- En relación con los datos personales, son obligaciones especiales de los sujetos obligados oficiales:

I.- Recabar datos personales sólo cuando sean ciertos, adecuados, pertinentes y no excesivos en relación con los propósitos de la información correspondiente;

II.- Informar y poner a disposición de los particulares, a partir del momento en el cual se recaben datos personales, del documento en donde se detallan los propósitos o finalidades de su utilización.

III.- Asentar los datos personales exactamente del modo en que hayan sido proporcionados.

IV.- Sustituir, rectificar o completar, de oficio o a petición del interesado, los datos personales que resultaren incompletos o inexactos, ya sea total o parcialmente; y

V.- Adoptar las medidas necesarias para garantizar la privacidad y seguridad de los datos personales y evitar su alteración, pérdida, transmisión o acceso no autorizado.

Artículo 34.- Se considerarán como confidenciales los datos personales referidos a una persona que ha fallecido, a los cuales únicamente podrán tener acceso y derecho a pedir su corrección, el albacea de la sucesión.

Cuando el titular de los datos personales haya fallecido, y el sujeto obligado reciba una solicitud de acceso o corrección de los mismos presentada por una persona distinta a la mencionada en los párrafos anteriores, la autoridad podrá solicitar el consentimiento del albacea.

Artículo 35.- Toda persona, que mediante identificación oficial demuestre su identidad, tendrá reconocimiento pleno por parte de los sujetos obligados, de sus derechos de acceso, rectificación, cancelación y oposición de sus datos personales en poder de éstos; pudiendo, con ello, saber si se está procesando información que le concierne, al solicitar una indagatoria y conseguir una reproducción inteligible de ella, a obtener las rectificaciones o cancelaciones que correspondan cuando los registros sean ilícitos, injustificados o inexactos, y a oponerse a su tratamiento cuando los datos se hayan recabado sin su consentimiento o demuestre la existencia de elementos o motivos suficientes para que se excluyan dichos datos del tratamiento a que eran sujetos. También tendrá el derecho a conocer los destinatarios, cuando esta información sea transmitida, permitiéndole conocer las razones que motivaron su pedimento, tal como lo establece el artículo 68 de los presentes lineamientos.

Para efectos del párrafo anterior, por identificación oficial se debe entender credencial de elector, licencia para conducir o pasaporte.

Presentada la solicitud de acceso, rectificación, cancelación u oposición de datos personales, la unidad de enlace dará observancia al procedimiento de atención a la misma, conforme lo establecido en el artículo 35 de la Ley de Acceso a la Información Pública del Estado de Sonora.

Artículo 36.- Sin perjuicio de lo que dispongan otras leyes, sólo los interesados o sus representantes podrán solicitar en las formas ya establecidas a una unidad de enlace, previa acreditación, que les proporcione los datos personales que obren en un sistema de datos personales. Aquélla deberá entregarle, en un plazo de diez días hábiles contados desde la presentación de la solicitud, en formato comprensible para el solicitante, la información correspondiente, o bien, le comunicará por escrito que ese sistema de datos personales no contiene los referidos al solicitante.

Artículo 37.- Las personas interesadas o sus representantes podrán solicitar, previa acreditación, ante la unidad de enlace o su equivalente, que modifiquen sus datos que obren en cualquier sistema de datos personales.

Con tal propósito, el interesado deberá entregar una solicitud de modificaciones a la unidad de enlace, donde se indique las modificaciones por realizarse y aporte la documentación que motive su petición. Asimismo, la unidad de enlace deberá entregar al solicitante, en un plazo de quince días hábiles desde la presentación de la solicitud, una comunicación que haga constar las modificaciones o bien, le informe de manera fundada y motivada, las razones por las cuales no procedieron las mismas.

Artículo 38.- No se considerará confidencial la información que se halle en los registros públicos o en fuentes de acceso público.

Artículo 39.- Los datos personales deberán ser invalidados cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recabados.

CAPITULO IV

Del procedimiento de clasificación y desclasificación

Artículo 40.- Los titulares de las unidades administrativas y/o, en su caso el comité de información podrán utilizar los formatos contenidos en el presente capítulo como modelo para señalar la clasificación de documentos o expedientes, sin perjuicio de que el sujeto obligado establezca los propios, los cuales deberán contener los elementos mínimos de la leyenda establecida en el lineamiento posterior.

Los documentos o expedientes públicos en su totalidad no llevarán leyenda o marca alguna y las anotaciones para la clasificación deberán asentarse en formato anexo al mismo.

Artículo 41.- La leyenda en los expedientes y documentos clasificados como reservados indicará:

I.- La fecha de la clasificación;

II.- El nombre de la unidad administrativa;

III.- El carácter de reservado;

IV.- Las partes o secciones reservadas, en su caso;

V.- El fundamento legal;

VI.- El período de reserva; y

VII.- La firma del titular de la unidad administrativa.

Artículo 42.- Los acuerdos de clasificación de información reservada deberán contener cuando menos lo siguiente:

I.- La fuente de la información; es decir, la referencia, origen, autoridad, ente o instancia de donde proviene esa información, denominación de quien la genera o a quién es atribuible su autoría.

II.- El daño que pudiera causar su divulgación; en cuyo caso deberá expresarse que de ser proporcionada o difundida al público, se estaría incumpliendo con la obligación que establece la ley en el sentido de que no debe divulgarse ni hacerse del conocimiento público, añadiendo las demás razones que el titular que clasifica considere aplicables al caso concreto relacionando dichas razones con algunas de las hipótesis del artículo 21 de la ley, así como de otras disposiciones jurídicas que sean aplicables.

III.- Las partes de los documentos que se reservan; en este caso, cuando solamente una parte de la documentación que forme parte de un expediente sea susceptible de clasificarse como reservada, únicamente procederá la clasificación parcial de dicho expediente en la parte relativa a esa información, debiéndose señalar en la carátula o portada del expediente, que él mismo cuenta con información clasificada, así como identificarse o señalizarse en lo individual cada uno de los documentos que se clasifiquen.

Al respecto, en la parte del expediente donde inicie la documentación susceptible de clasificación, o tratándose de documentación individual que no forme parte de expedientes, deberá anteponerse una carátula o portada en la que se asiente en original el acuerdo de clasificación, el cual llevará la leyenda alusiva al mismo en una o más fojas, y el cual deberá reunir los requisitos que para tal efecto se establecen.

Asimismo, al final del documento que sea clasificado, se anexará una contraportada en la que se indique la razón de que el documento o documentos que anteceden fueron clasificados en términos del acuerdo respectivo que obra en la portada.

En los casos en los que la totalidad de los documentos que formen parte de un expediente sean clasificados, se hará la anotación correspondiente en la carátula o portada del mismo, sin que se realice ningún señalamiento a cada uno de los documentos específicos.

Asimismo, mediante un solo acuerdo podrá llevarse a cabo la clasificación de un conjunto o grupo de información que obre en un archivo, base de datos, dispositivo magnético o cualquier otro tipo de almacenamiento, siempre y cuando la totalidad de esa información cumpla con los requisitos para ser considerada como reservada y se relacione en el índice correspondiente el contenido de toda la información que obre en alguno de los medios de almacenamiento antes mencionados.

IV.- El plazo de reserva; dicho requisito aplica únicamente para la información clasificada como reservada, ya que la información confidencial se mantiene

permanentemente restringida y aún con el paso del tiempo no es susceptible de ser difundida, salvo la excepción contemplada en el artículo 36.

Para el caso de la Información reservada, se deberá asentar el período de reserva por el plazo necesario para que la información permanezca con ese carácter, siempre y cuando sea previsible dicho término de tiempo; en caso contrario, cuando no pueda estimarse el plazo necesario para que la información se mantenga como tal, por regla general deberá asentarse el plazo de diez años previsto en el artículo 25 de la ley.

Artículo 43.- La falta de alguno de los requisitos señalados en el lineamiento anterior, no implica la pérdida del carácter de reservado de la información, por lo que los titulares de las unidades administrativas de los sujetos obligados y/o, en su caso el comité de información podrán subsanar los requisitos que se hubiesen omitido.

Artículo 44.- Una vez que se lleve a cabo la clasificación de la información por parte de los titulares de las unidades administrativas y/o, en su caso el comité de información, cada uno deberá elaborar un índice en el que se señale por grupos de temas, los expedientes clasificados únicamente como reservados, debiéndose observar para ello, los requisitos establecidos en el artículo 26 de la ley.

En ese sentido, los titulares de las unidades administrativas y/o, en su caso el comité de información llevarán a cabo cada mes la actualización de dichos índices, con independencia de que semestralmente remitirán al Instituto dichas actualizaciones.

Artículo 45.- Tratándose de información clasificada como reservada, los titulares de las unidades administrativas que tengan a su cargo o bajo su posesión la información solicitada, deberán revisar el acuerdo de clasificación al momento de la recepción de la solicitud, con el fin de verificar que subsistan las causas que dieron origen o que motivaron la clasificación.

Artículo 46.- Los sujetos obligados elaborarán los formatos a que se refiere este capítulo en medios impresos, electrónicos, mecánicos, entre otros, debiendo ubicarse dicho formato en la esquina superior derecha del documento.

Artículo 47.- El formato para señalar la clasificación de documentos que se consideran reservados en todo o en parte, es el siguiente:

I.- “Sello oficial o logotipo de la dependencia o entidad”	**II.- fecha de clasificación: a)** **unidad administrativa: b)** **reservada: c)** **período de reserva: d)** **fundamento legal: e)** **ampliación del período de reserva: f)** **rúbrica del titular de la unidad administrativa: g)** **fecha de desclasificación: h)** **rúbrica y cargo del servidor público: i)**

I.- En la esquina superior izquierda del formato se ubicará el sello oficial o logotipo del sujeto obligado que se trate.

II.- Del lado derecho del formato se anotarán los siguientes medios de identificación:

a) Se anotará la fecha en que se clasifica el documento;

b) Se señalará el nombre de la unidad administrativa de la cual es titular quien clasifica;

c) Se indicarán, en su caso, las partes o páginas del documento que se clasifican como reservadas. Si el documento fuera reservado en su totalidad, se anotarán todas las páginas que lo conforman;

d) Se anotará el número de años por los que se mantendrá el documento o las partes del mismo con el carácter de reservado;

e) Se señalará el nombre del o de los ordenamientos jurídicos, el o los artículos, fracción(es) y párrafo(s) con base en los cuales se sustenta la reserva;

f) En caso de haber solicitado la ampliación del período de reserva originalmente establecido, se deberá anotar el número de años por los que se amplía la reserva;

g) Firma autógrafa de quien clasifica; y en su caso;

h) Se anotará la fecha en que la información se desclasifica; y

i) Firma autógrafa de quien desclasifica.

Artículo 48.- El expediente del cual formen parte los documentos a que se refiere el lineamiento anterior, únicamente llevará en su carátula la especificación de que contiene partes o secciones reservadas.

Artículo 49.- El formato para señalar la clasificación de expedientes que por su naturaleza sean en su totalidad reservados, es el siguiente:

I.- "Sello oficial o logotipo de la dependencia o entidad"

II.-
fecha de clasificación: a)
unidad administrativa: b)
período de reserva: c)
fundamento legal: d)
ampliación del período de reserva: e)
rúbrica del titular de la unidad administrativa: f)
fecha de desclasificación: g)
partes o secciones reservadas: h)
rúbrica y cargo del servidor público: i)

I.- En la esquina superior izquierda del formato se ubicará el sello oficial o logotipo del sujeto obligado que se trate.

II.- Del lado derecho del formato se anotarán los siguientes medios de identificación:

a) Se anotará la fecha en que se clasifica el documento;

b) Se señalará el nombre de la unidad administrativa de la cual es titular quien clasifica;

c) Se anotará el número de años por los que se mantendrá el expediente con el carácter de reservado;

d) Se señalará el nombre del o de los ordenamientos jurídicos, el o los artículos, fracción(es) y párrafo(s) con base en los cuales se sustenta la reserva;

e) En caso de haber solicitado la ampliación del período de reserva originalmente establecido, se deberá anotar el número de años por los que se amplía la reserva;

f) Firma autógrafa de quien clasifica;

g) Se anotará la fecha en que la información se desclasifica;

h) En caso de que una vez desclasificado el expediente, subsistan partes o secciones del mismo reservadas, se señalará este hecho; y

i) Firma autógrafa de quien desclasifica.

Artículo 50.- Los documentos que integren un expediente reservado en su totalidad no deberán marcarse en lo individual, tal es el caso, entre otros, de los expedientes a que se refiere la fracción VI del artículo 21 de la ley.

Si existieran en dichos expedientes documentos marcados como clasificados, que hayan sido enviados por otro sujeto obligado, prevalecerán sobre éstos, la fecha de clasificación y el período de reserva que obre en la carátula del expediente.

Una vez desclasificados los expedientes a que se refiere el primer párrafo de este numeral, si existieren documentos que tuvieran el carácter de reservados, deberán ser marcados de conformidad con el artículo 49 de los presentes lineamientos.

Artículo 51.- El acuerdo para desclasificar la información reservada a que se refiere la fracción II del artículo 15 de los presentes lineamientos, deberá contener lo siguiente:

I.- Fecha de desclasificación;

II.- El nombre de la Unidad Administrativa;

III.- Las causas que dieron origen a la desclasificación, atendiendo las circunstancias de modo, tiempo y lugar; y

IV.- Rúbrica y cargo de los integrantes del comité de información o del servidor público que desclasifica.

CAPÍTULO V
De la protección de los datos personales

Sección Primera
Disposiciones generales

Artículo 52.- Los datos personales son irrenunciables, intransferibles e indelegables, por lo que los sujetos obligados no podrán comunicar a terceros, ni difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información. Esta obligación persistirá en los términos establecidos en el artículo 12 de los presentes lineamientos.

Artículo 53.- Los sistemas de datos personales podrán distinguirse entre físicos y automatizados, definiéndose cada uno de ellos de la siguiente forma:

I.- Físicos: Conjunto ordenado de datos que para su tratamiento están contenidos en registros, manuales, impresos, sonoros, magnéticos, visuales u holográficos; y,

II.- 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.

Los datos personales contenidos en los sistemas se clasificarán, de manera enunciativa, más no limitativa, de acuerdo a las siguientes categorías:
a) Datos identificativos: El nombre, domicilio, teléfono particular, teléfono celular, firma, Clave Única de Registro de Población (CURP), Matrícula del Servicio Militar Nacional, número de pasaporte, lugar y fecha de nacimiento, nacionalidad, edad, fotografía, y demás análogos;
b) Datos electrónicos: Las direcciones electrónicas, tales como: el correo electrónico no oficial, dirección IP (Protocolo de Internet), dirección MAC (dirección Media Access Control o dirección de control de acceso al medio), así como el nombre del usuario, contraseñas, firma electrónica; o cualquier otra información empleada por la persona para su identificación en Internet u otra red de comunicaciones electrónicas;
c) 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;
d) 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 análogas;

e) Datos sobre procedimientos administrativos y/o jurisdiccionales: La información relativa a una persona que se encuentre incluida en expedientes de procedimientos administrativos o jurisdiccionales en materia laboral, civil, penal, fiscal, administrativa o de cualquier otra rama del Derecho;
f) Datos académicos: Trayectoria educativa, calificaciones, certificados y reconocimientos, y demás análogos;
g) Datos de tránsito y movimientos migratorios: Información relativa al tránsito de las personas dentro y fuera del país, así como información migratoria;
h) 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, así como el estado físico o mental de la persona;
i) Datos biométricos: huellas dactilares, ADN, geometría de la mano, características de iris y retina, y demás análogos; y,
j) Datos especialmente protegidos o sensibles: origen étnico o racial, características morales o emocionales, ideología y opiniones políticas, creencias, convicciones religiosas, filosóficas y preferencia sexual, y demás análogas.

Artículo 54.- La posesión de un sistema de datos personales deberá obedecer exclusivamente a las atribuciones legales o reglamentarias de cada sujeto obligado y deberán obtenerse a través de los medios previstos en dichas disposiciones.

Los datos personales deberán tratarse únicamente para la finalidad que fueron obtenidos. Dicha finalidad debe ser determinada y legítima.

Sección Segunda
Principios rectores en la protección de datos personales

Artículo 55.- Los sistemas de datos personales deberán constituirse de tal forma que permitan el ejercicio de los derechos de acceso, rectificación, cancelación y oposición previstos en la Ley.

Artículo 56.- Se deberán adoptar las medidas necesarias para garantizar la integridad, confiabilidad, confidencialidad y disponibilidad de los datos personales mediante acciones que eviten su alteración, pérdida, transmisión y acceso no autorizado.

Artículo 57.- El tratamiento de datos personales deberá ser cierto, adecuado, pertinente y no excesivo, respecto de las atribuciones legales de la dependencia o entidad que los posea.

Artículo 58.- En el tratamiento de datos personales, los sujetos obligados deberán observar los principios de licitud, calidad, confidencialidad, temporalidad, consentimiento, seguridad y disponibilidad que señala el artículo 32 de la Ley.

Artículo 59.- Se deberá hacer del conocimiento del titular de los datos, al momento de recabarlos y de forma escrita, el fundamento y motivo de ello, así como los propósitos para los cuales se tratarán dichos datos.

Artículo 60.- A efecto de determinar si la información que posee un sujeto obligado constituye un dato personal, deberán agotarse las siguientes condiciones:
a) Que la misma sea concerniente a una persona física, identificada o identificable; y,
b) Que la información se encuentre contenida en sus archivos.

Artículo 61.- Los datos personales serán debidamente custodiados, quedando la responsabilidad de ello a los titulares de las unidades administrativas que los contengan; asimismo, los responsables, encargados y usuarios de los sistemas de datos personales deberán garantizar el manejo cuidadoso en su tratamiento.

Artículo 62.- 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 72 de los presentes lineamientos.

Sección Tercera
Del tratamiento cierto, adecuado, pertinente y no excesivo

Artículo 63.- A efecto de cumplir con el principio de calidad a que se refiere el artículo 58 de los presentes lineamientos en correlación con el 32 de la Ley, se considera que el tratamiento de datos personales es:
a) Cierto: Cuando los datos personales se encuentran incorporados de manera tal que guarden concordancia con la veracidad de la información.
b) Adecuado: Cuando se observan las medidas de seguridad aplicables que garanticen su resguardo y salvaguarda;
c) Pertinente: Cuando es realizado para el cumplimiento de las atribuciones de los sujetos obligados que los hayan recabado y por el personal autorizado; y,
d) No excesivo: Cuando la información solicitada al titular de los datos es estrictamente la necesaria para cumplir con los fines para los cuales se hubieran recabado.

Artículo 64.- En caso de que los responsables, encargados o usuarios detecten que hay datos personales inciertos, deberán de oficio, actualizarlos en el momento en que tengan conocimiento de la inexactitud de los mismos, siempre que posean los documentos que justifiquen la actualización y que dicha modificación no traiga como consecuencia que el titular de los datos se vea afectado por dicha situación.

Artículo 65.- Los documentos que contengan datos personales que hayan sido objeto de tratamiento y no contengan valores históricos, científicos, estadísticos o contables, deberán ser dados de baja por los sujetos obligados mediante la destrucción documental regulada en los artículos 67 y 68 de la Ley de Acceso a la Información Pública del Estado de Sonora, o bien, los que contengan dichos valores serán objeto de transferencias secundarias, de conformidad con lo establecido por la Ley No. 167 que

regula la Administración de Documentos Administrativos e Históricos del Estado, teniendo en cuenta los siguientes plazos:
a) El que se haya establecido en el formato físico o electrónico por el cual se recabaron;
b) El establecido por las disposiciones aplicables;
c) El establecido en los convenios formalizados entre una persona y la dependencia o entidad; y,
d) El señalado en los casos de transmisión.

Para el supuesto de que existan dos o más plazos se atenderá al que asegure la disposición de los datos personales.

Artículo 66.- Los datos personales sólo serán tratados en sistemas de datos personales que reúnan las condiciones mínimas de seguridad establecidas en estos lineamientos y las demás disposiciones aplicables.

Artículo 67.- En el momento en que se recaben datos personales, los sujetos obligados deberán hacer del conocimiento al titular de los datos tanto en los formatos físicos como en los electrónicos utilizados para ese fin, lo siguiente:
a) La mención de que los datos recabados serán protegidos en términos de lo dispuesto por la Ley;
b) El fundamento legal para ello; y,
c) El objeto y la finalidad del Sistema de Datos Personales.

Artículo 68.- Sin perjuicio de que los sujetos obligados elaboren sus propios formatos para informar al titular de los datos lo establecido por el artículo anterior, podrán utilizar el siguiente modelo:
"Los datos personales recabados serán protegidos, incorporados y tratados en el Sistema de Datos Personales **(indicar nombre),** con fundamento en (indicar) y cuya finalidad es (describirla); el cual fue registrado en el Directorio Estatal de Sistemas de Datos Personales ante el Instituto de Transparencia Informativa del Estado de Sonora **(www.transparenciasonora.org),** y podrán ser transmitidos a **(indicar),** con la finalidad de **(indicar),** además de otras transmisiones previstas en la Ley. La Unidad Administrativa responsable del Sistema de Datos Personales es **(indicarlo),** y la dirección donde el interesado podrá ejercer los derechos de acceso, rectificación, cancelación y oposición ante la misma es **(indicarla).** Lo anterior se informa en cumplimiento del artículo 67 de los Lineamientos para el manejo de la información restringida y la protección de los datos personales en posesión de los Sujetos Obligados del Estado de Sonora, emitidos por el Instituto de Transparencia Informativa del Estado de Sonora".

Artículo 69.- Los sujetos obligados que recaben datos personales a través de un servicio de orientación telefónica, u otros medios o sistemas, deberán establecer un mecanismo por el que se informe previamente a los particulares que sus datos personales serán recabados, la finalidad de dicho acto así como el tratamiento al cual serán sometidos, cumpliendo con lo establecido en el artículo 67 de los presentes Lineamientos.

Artículo 70.- El tratamiento de datos personales para fines estadísticos deberá efectuarse mediante la disociación de los datos, de conformidad con la fracción II del artículo 2 de los presentes lineamientos, la Ley Federal en la materia y las demás disposiciones aplicables.

Artículo 71.- Cuando se contrate a terceros para que realicen el tratamiento de datos personales, deberá estipularse en el contrato respectivo, la implementación de medidas de seguridad y custodia previstas en estos lineamientos, en la normatividad aplicable a las dependencias y entidades contratantes, así como la imposición de penas convencionales por su incumplimiento.

Sección Cuarta
De la transmisión de los datos

Artículo 72.- Los sujetos obligados podrán transmitir datos personales sin el consentimiento del titular de los datos, en los casos previstos en el artículo 31 de la Ley de Acceso a la Información Pública del Estado de Sonora. Asimismo, deberán otorgar el acceso a aquellos datos que no se consideran como confidenciales por ubicarse en los supuestos establecidos y aplicables para la información pública básica tal y como se establece en dicha Ley.

Artículo 73.- Para la transmisión de los datos personales, el consentimiento del titular de los mismos deberá emitirse por escrito incluyendo la firma autógrafa y la copia de su 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 o firmas electrónicas. El servidor público encargado de recabar el consentimiento del titular de los datos para la transmisión de los mismos, deberá entregar a éste, en forma previa, un formato de la autorización para la transmisión de datos personales y proporcionara además la información suficiente acerca de las implicaciones de otorgar su consentimiento.

Sección Quinta
Del Directorio Estatal de Sistemas de Datos Personales

Artículo 74.- El Instituto implementará el Directorio Estatal de Sistemas de Datos Personales, mismo que debe ser actualizado de forma semestral.

Artículo 75.- Los Responsables deberán registrar e informar al Instituto, dentro de los primeros treinta días hábiles de cada seis meses, lo siguiente:
a) Los sistemas de datos personales; y,
b) Cualquier modificación sustancial o cancelación de dichos sistemas.

Artículo 76.- El registro del Sistema de Datos Personales en el Directorio deberá contener los siguientes datos:
a) Nombre del sistema;
b) Unidad administrativa en la que se encuentra el sistema;
c) Nombre del responsable del sistema;
d) Cargo del Responsable;
e) Teléfono y correo electrónico del Responsable;
f) Finalidad del sistema; y,
g) Normatividad aplicable.

Artículo 77.- Los sujetos obligados oficiales deberán establecer un vínculo en sus sitios de Internet al "Directorio Estatal de Sistemas de Datos Personales".

Sección Sexta
De la seguridad de los sistemas de datos personales

Artículo 78.- Para proveer seguridad a los sistemas de datos personales, los sujetos obligados por conducto de los titulares de las unidades administrativas en donde se implementen dichos sistemas, deberán observar las medidas siguientes:

I. Establecer la conformación del Comité de Información para la emisión de criterios específicos sobre el manejo, mantenimiento, seguridad y protección de los sistemas de datos personales, los cuales no podrán contravenir lo dispuesto por los presentes lineamientos;

II. Designar a los Responsables;

III. Proponer al Comité de Información la difusión de la normatividad entre el personal involucrado en el manejo de los sistemas de datos personales; y,

IV. Proponer al Comité de Información en coordinación con el Instituto, la elaboración de un plan de capacitación en materia de seguridad de datos personales dirigida a los Responsables, Encargados y Usuarios.

Artículo 79.- En cada sujeto obligado, el Comité de Información coordinará y supervisará las acciones de promoción del manejo, mantenimiento, seguridad y protección de los sistemas de datos personales, así como de la integridad, confiabilidad, disponibilidad y exactitud de la información contenida en dichos registros.

Artículo 80.- La documentación generada para la implementación, administración y seguimiento de las medidas de seguridad administrativa, física, técnica y tecnológica de los sistemas de datos personales tendrá el carácter de información reservada y será de acceso restringido.

El personal que tenga acceso a dicha documentación deberá evitar que ésta sea divulgada, a efecto de no comprometer la integridad, confiabilidad, confidencialidad y disponibilidad de los sistemas de datos personales así como del contenido de éstos.

Artículo 81.- 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 o acceso no autorizado;
b) Autorizar expresamente, en los casos en que no esté previsto por un instrumento jurídico, a Encargados y Usuarios, y llevar una relación actualizada de las personas que tengan acceso a los sistemas de datos personales que se encuentran en soporte físico; e,
c) Informar al Comité de Información los nombres de los Encargados y Usuarios.

Artículo 82.- Los sujetos obligados deberán:

I. Asignar un espacio físico y/o virtual, seguro y adecuado para la operación de los sistemas de datos personales;

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

III. Contar con al menos dos lugares distintos, que cumplan con las condiciones de seguridad especificadas en estos Lineamientos, destinados a almacenar medios de respaldo de sistemas de datos personales;

IV. Realizar procedimientos de control, registro de asignación y baja de los equipos de cómputo a los Usuarios que utilizan datos personales, considerando al menos las siguientes actividades:
a) Si es asignación, configurarlo con las medidas de seguridad necesarias, tanto a nivel operativo como de infraestructura; y,
b) Verificar y llevar un registro del contenido del equipo para facilitar los reportes del Usuario que lo recibe o lo entrega para su baja.

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

VI. Implantar medidas de seguridad para el uso de los dispositivos electrónicos y físicos de salida, así como para evitar el retiro no autorizado de los mismos fuera de las instalaciones de los sujetos obligados; y,

VII. En el caso de requerirse disponibilidad crítica de datos, instalar y mantener el equipamiento de cómputo, eléctrico y de telecomunicaciones necesarios. Además, realizar respaldos que permitan garantizar la continuidad de la operación.

Artículo 83.- 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; y,

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.

Artículo 84.- 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 o al sitio donde se ubican los mismos.

Artículo 85.- El documento mencionado en el precepto 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 estos 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 de información contenida en el sistema de datos personales;
c) Procedimientos de creación de copias de respaldo y de recuperación de los datos;
d) Bitácoras de acciones llevadas a cabo en el sistema de datos personales;
e) Procedimiento de notificación, gestión y respuesta ante incidentes; y,
f) Procedimiento para la cancelación de un registro de datos personales.

El contenido del documento deberá revisarse y, en su caso, actualizarse anualmente.

Artículo 86.- 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.

Artículo 87.- 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. Registro 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.

Artículo 88.- 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 podrán establecer manuales de procedimientos y de organización para el tratamiento de datos personales, mismos que observaran obligatoriamente los responsables, encargados o usuarios de los sistemas de datos personales llevando a cabo, en forma adicional, las siguientes medidas:

I. Contemplar la utilización de espacios externos seguros para guardar de manera sistemática los respaldos de las bases de datos de los sistemas de datos personales;

II. Emplear 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:

III. Aplicar mecanismos de revisión, llevando 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 de Control Interno;

IV. Garantizar que el personal encargado del tratamiento de datos personales, sólo tenga acceso a las funciones autorizadas del sistema de datos personales según su perfil de usuario, teniendo como apoyo la rastreabilidad de operaciones;

V. Aplicar procedimientos de respaldos de bases de datos y realizar pruebas periódicas de restauración;

VI. Llevar control de inventarios y clasificación de respaldos de los datos personales;

VII. Llevar el control 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 establezca el sujeto obligado;

VIII. Garantizar que durante la transmisión física o virtual de datos personales y el transporte de los soportes de almacenamiento, los datos no sean accesados, reproducidos, alterados o suprimidos sin autorización;

IX. Aplicar procedimientos para la destrucción de medios de almacenamiento de respaldo obsoletos que contengan datos personales, y consiguiente migración a medios de almacenamiento actuales;

X. En los casos en que la operación del sistema sea externa, se deberá convenir con el proveedor del servicio que la dependencia o entidad tenga la facultad de verificar que se respete la integridad, confiabilidad, confidencialidad y disponibilidad de los datos personales; y 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;

XI. Diseñar planes de contingencia que garanticen la continuidad de la operación de los sistemas de datos y realizar pruebas de eficiencia de los mismos; y,

XII. Cualquier otra medida que garantice el cumplimiento de los principios de protección de datos personales señalados en la Sección Segunda de estos lineamientos.

Sección Séptima
Del Instituto

Artículo 89.- Los sujetos obligados podrán solicitar al Instituto la revisión y supervisión a los lugares en los que se encuentran y operan los sistemas de datos personales, poniendo a disposición de sus servidores públicos la documentación técnica y administrativa de dichos sistemas, con el objeto de diagnosticar que se cumpla con la Ley y los presentes lineamientos.

Artículo 90.- En caso de que el Instituto determine que algún servidor público pudo haber incurrido en responsabilidades por el incumplimiento de estos lineamientos, deberá dar conocimiento al Órgano de Control Interno correspondiente, a efecto de que determine lo conducente, con base a la Ley de Responsabilidades de los Servidores Públicos del Estado y de los municipios.

TRANSITORIOS

PRIMERO.- Los presentes lineamientos entrarán en vigor al día siguiente de su publicación en el Boletín oficial del Gobierno del Estado.

SEGUNDO.- Se derogan todas las disposiciones reglamentarias existentes en las entidades públicas que se opongan a lo dispuesto en los presentes lineamientos, los cuales fueron dados en la ciudad de Hermosillo, Sonora a 29 del mes de mayo del año dos mil seis por los vocales integrantes del Instituto de Transparencia Informativa del Estado de Sonora, C. P. Conrado Jaime Samaniego Villasana, C. P. Ricardo Hurtado Ibarra y Lic. Francisco Cuevas Sáenz.

FECHA DE APROBACIÓN: **2006/05/29**
FECHA DE PUBLICACIÓN: **2006/07/10**
PUBLICACIÓN OFICIAL: **3, SECCIÓN III, BOLETÍN OFICIAL**
INICIO DE VIGENCIA: **2006/07/11**

Reformada en 2012/03/29, Boletín Oficial 26, Sección I.

ARTÍCULO TRANSITORIO DE LOS LINEAMIENTOS
(Publicados en 2012/03/29, B.O. 26, Sección I)

Que reforma los lineamientos de fecha 15 de marzo de 2012, con modificaciones y adiciones de los siguientes preceptos: Se modifican, el nombre de los presentes lineamientos; los artículos 1; 2; 3; 4; 6; 8; 9; 11; 12; la fracción III del 15; las fracciones I y II del 16; el inciso c) de la fracción I del 30; los incisos b), h), o) y p) del 31; la fracción I del 33; 35; 40; 43 y 44. Se adicionan, ocho fracciones al artículo 2; un segundo párrafo al 4; se crea un artículo 4 bis; un último párrafo al 22; dos incisos al 31; dos últimos párrafos al 35; y, un capítulo V (quinto) con 39 artículos que van desde el 52 al 90, y el cual se denomina "De la protección de los datos personales", mismo que se compone por las secciones, primera "Disposiciones generales"; segunda "Principios rectores en la protección de datos personales"; tercera "Del tratamientos cierto, adecuado, pertinente y no excesivo"; cuarta "De la transmisión de los datos"; quinta "Del Directorio Estatal del Sistema de Datos Personales"; sexta "De la seguridad de los datos personales" y, séptima "Del Instituto".

Único. La presente reforma entrará en vigor al día siguiente de su publicación en el Boletín Oficial del Estado de Sonora, con excepción de las obligaciones derivadas de la sección sexta, denominada "De la seguridad de los datos personales", para lo cual, se determina un plazo de tres años a fin de que los sujetos obligados del Estado hagan las modificaciones y adecuaciones necesarias para el cumplimiento de dichas disposiciones normativas.