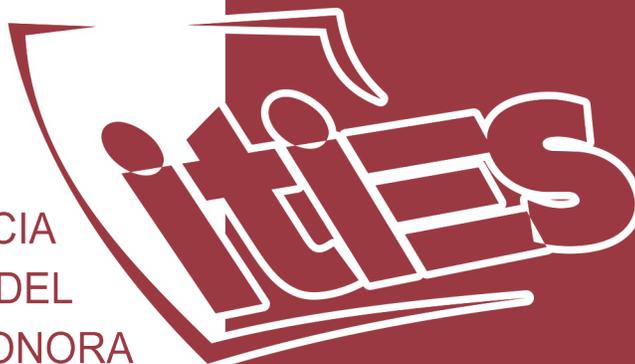


INSTITUTO DE
TRANSPARENCIA
INFORMATIVA DEL
ESTADO DE SONORA



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

Biblioteca
DE LA TRANSPARENCIA

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

CAPÍTULO I DISPOSICIONES GENERALES	109	SECCIÓN SEGUNDA PRINCIPIOS RECTORES EN LA PROTECCIÓN DE DATOS PERSONALES	130
SECCIÓN PRIMERA DE LA CLASIFICACIÓN	109	SECCIÓN TERCERA DEL TRATAMIENTO CIERTO, ADECUADO, PERTINENTE Y NO EXCESIVO	131
SECCIÓN SEGUNDA DE LAS DESCLASIFICACIÓN	113	SECCIÓN CUARTA DE LA TRANSMISIÓN DE LOS DATOS	133
CAPÍTULO II DE LA INFORMACIÓN RESERVADA	114	SECCIÓN QUINTA DEL DIRECTORIO ESTATAL DE SISTEMAS DE DATOS PERSONALES	133
CAPÍTULO III DE LA INFORMACIÓN CONFIDENCIAL	121	SECCIÓN SEXTA DE LA SEGURIDAD DE LOS SISTEMAS DE DATOS PERSONALES	134
CAPÍTULO IV DEL PROCEDIMIENTO DE CLASIFICACIÓN Y DESCLASIFICACIÓN	125	SECCIÓN SÉPTIMA DEL INSTITUTO	138
CAPÍTULO V DE LA PROTECCIÓN DE LOS DATOS PERSONALES	129	TRANSITORIOS	138
SECCIÓN PRIMERA DISPOSICIONES GENERALES	129		

**LINEAMIENTOS GENERALES PARA LA CUSTODIA
Y MANEJO DE LA 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 y de Protección de Datos Personales del 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 modificarán, 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 el artículo 3 de la Ley de Acceso a la Información Pública y de Protección de Datos Personales del Estado de Sonora, así como 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;
- 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;
- XI. **Prueba de Daño:** Carga de los entes públicos para demostrar que la divulgación de cierta información lesiona el interés jurídicamente protegido por la Ley, y que el daño que puede producirse con la publicidad de dicha información es mayor que el beneficio de conocerla;
- XII. **Ley:** Ley de Acceso a la Información Pública y de Protección de Datos Personales del Estado de Sonora, y
- XIII. **Versión pública:** Documento del que se elimina la información y/o datos clasificados como reservados o confidenciales, a fin de permitir su libre acceso.

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.

ARTÍCULO 5.- 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;
- 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 6.- 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, por lo cual no requiere de acuerdo expreso.

En ningún caso los sujetos obligados podrán clasificar documentos como de acceso restringido antes de que se genere la información.

ARTÍCULO 7.- 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 8.- En el caso de información reservada, deberá establecerse el período de reserva, el que podrá ser por diez años, prorrogables excepcionalmente con anterioridad a su conclusión, en caso de subsistir las causas que originaron su clasificación o que aparezcan otras de igual o mayor gravedad; asimismo, 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 último párrafo del artículo

41 de los presentes lineamientos y la legislación aplicable.

Se exceptúa de los plazos establecidos en este artículo, la información a que hacen referencia los artículos 29 y 32 de estos Lineamientos, cuyo plazo estará condicionado a lo establecido en las leyes especiales que las regulen.

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

ARTÍCULO 9.- 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; por lo tanto, la información deberá ser clasificada por el sujeto obligado antes de dar respuesta a una solicitud de acceso a la información.

ARTÍCULO 10.- 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 11.- 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 o verificables, donde pueda identificarse una alta probabilidad de dañar el interés público protegido conforme a los supuestos que se establecen en el artículo 21, y demás relativos de la Ley.

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, artículos, párrafos, fracciones o incisos 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 12.- 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, pero siempre antes de dar respuesta a dicha solicitud.

ARTÍCULO 13.- 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.

Artículos 14.- 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 15.- 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 16.- Los expedientes y documentos clasificados como reservados podrán desclasificarse cuando:

- I. Haya transcurrido el período de reserva que indique el acuerdo;
- 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 siete 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 sólo transcurso del tiempo, sin necesidad de resolución o acto administrativo alguno.

ARTÍCULO 17.- 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 sólo transcurso del tiempo por el que originalmente fue clasificada, salvo que se amplié el período.

Los sujetos obligados elaborarán un listado de información que habrá de desclasificarse al momento que se cumpla el período de reserva, mismo que deberá incluirse en el informe remitido al Instituto, previsto por el artículo 26 de la Ley.

ARTÍCULO 18.- 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

Artículos 19.- Se clasificará como reservada la información cuando se ponga en riesgo la seguridad nacional, la seguridad pública 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 aquella 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 pone 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, entendiéndose 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; asimismo, aquellas acciones que, por sus propias características, de ser divulgadas pongan en riesgo su realización, ya sea 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 en situación vulnerable la integridad de las fuerzas armadas de la federación, de las policías federales, estatales y municipales; las operaciones de control migratorio, atentándose 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) Menoscar 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 20.- La información se clasificará como reservada cuando, con su difusión, pudiera ponerse en riesgo la vida, la seguridad o la salud de cualquier persona, así como el desarrollo de las investigaciones reservadas. Se podrá clasificar como reservada en los siguientes supuestos:

I. Cuando la difusión de la información pueda menoscar la capacidad de las autoridades de seguridad pública para preservar y resguardar la vida o la salud de las personas, relacionada con:

- a) El personal de seguridad, tales como nombres, adscripciones, asignaciones, bitácoras, roles de servicios, fotografías, cargos y funciones, en especial de los integrantes de los cuerpos policiales y de seguridad, excepto su remuneración. La información del personal de seguridad deberá proporcionarse de manera disociada, de tal manera que no permita identificar si se cuenta o no con asignación para proteger a determinadas personas;
- b) La tecnología aplicada a la tarea de seguridad pública y que permita relacionarla directamente con determinado personal operativo y/o su asignación para la protección de determinada persona; y
- c) Períodos y horario de prestación de servicio.

II. Aquella que pudiera repercutir en alguna afectación al desarrollo de las investigaciones reservadas, en caso de que la difusión de la información pueda impedir u obstruir las investigaciones que realizan los sujetos que intervienen en las diversas etapas de los procesos judiciales, administrativos o arbitrales, así como aquellos que se sustancian ante tribunales internacionales; 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 directamente relacionadas con la seguridad de funcionarios públicos, la procuración e impartición de justicia, así como las 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 21.- Se clasificará como reservada en los términos del artículo 21, fracción III de la Ley, cuando se cause un serio perjuicio a:

- I. 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. 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.
- III. Estropear o dificultar las actividades de verificación del cumplimiento de las leyes, así como 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 a 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 la 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 tal 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 22.- 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 quien solicite la información acorde a los ordenamientos legales que rijan en cada caso; y
- III. Cuando se trate de juicios que por su naturaleza sean de interés público a consideración de los tribunales que conozcan del asunto.

Cuando existan procedimientos accesorios al juicio principal, las partes que integren este último podrán consultar en todo momento la información relativa a los primeros, siempre de acuerdo a las leyes procesales aplicables.

ARTÍCULO 23.- La información se clasificará como reservada en los términos del artículo 21, fracción IV de la Ley, cuando ésta expresamente así la considere, debiendo encuadrar el caso concreto a la hipótesis que le resulte aplicable, considerando que:

- I. La Ley estatal vigente le otorga ese carácter;
- II. Son aquellos instrumentos jurídicos que suscriban los gobiernos estatal y municipales con la federación, siempre y cuando el objeto de dicho acuerdo estipule cláusula de confidencialidad, y;
- III. La que los sujetos obligados reciban con tal carácter de parte de otros gobiernos u organismos.

ARTÍCULO 24.- La información se clasificará como reservada en los términos de la fracción V del artículo 21 de la Ley, siempre que se trate de expedientes judiciales o de los procedimientos

administrativos seguidos en forma de juicio, incluidos los laborales, que no hayan causado estado, tales como:

- I. Procesos y procedimientos sustanciados ante los tribunales judiciales y administrativos del Estado;
- II. Procedimientos de carácter laboral;
- III. Procedimientos de queja ante las áreas de inspección general de policía, asuntos internos o comisión de honor y justicia; y
- IV. Los procedimientos de queja ante la Comisión Estatal de Derechos Humanos.

En todos los casos se deberá fundamentar y motivar, informando del estado procesal que guarda.

Se entiende que una resolución es definitiva una vez que las sentencias o resoluciones de mérito no puedan ser modificadas o revocadas por ningún medio de defensa ordinario o extraordinario.

Para el caso de los procedimientos administrativos seguidos en forma de juicio en los que no se hubiere dictado una resolución definitiva, pero que hayan sido archivados de manera definitiva por medio de un acuerdo, éstos no se considerarán como información reservada, y por lo tanto las actuaciones que deriven de los mismos será información de acceso público, ya que se les tendrá por concluidos.

ARTÍCULO 25.- Se clasificará la información como reservada cuando tratándose de procedimientos de responsabilidad de los servidores públicos, quejas y denuncias tramitadas ante los órganos de control, no se haya dictado la resolución administrativa definitiva, esto es, que existan aún recursos administrativos y/o legales a ejercer.

ARTÍCULO 26.- La información se clasificará como reservada cuando contenga las opiniones, recomendaciones o puntos de vista que formen parte del proceso deliberativo de los servidores públicos, en tanto pueda influenciar un proceso de toma de decisiones afectando el interés público y 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 impugnada, 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 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 aun cuando formalmente no sean objetos de prueba en un juicio o procedimiento en que éstos intervengan como parte, por relacionarse con tales diligencias puedan afectar la actuación de la autoridad en materia de controversias legales.

ARTÍCULO 28.- La información se clasificará como reservada cuando, con su difusión, se pueda

generar una ventaja personal indebida en perjuicio de un tercero o de los sujetos obligados.

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 la revelación de la información, perjudique o lesione intereses generales o particulares, por cuanto quien acceda a ella de manera previa pudiera obtener un beneficio indebido e ilegítimo. Respecto de este supuesto, al clasificar la información como reservada deberán precisarse, de manera fundada y motivada, los intereses generales o particulares que pudieran verse lesionados; y
- II. Cuando se difunda información que comprenda hechos y actos de carácter económico, contable, jurídico o administrativo relativos a una persona que en cumplimiento de una disposición legal, entregue a cualquier sujeto obligado, siempre y cuando contenga detalles sobre el manejo de su actividad, verse sobre el proceso de toma de decisiones o información que pudiera afectar sus negociaciones, acuerdos de los órganos de administración, políticas de dividendos y sus modificaciones o actas de asamblea.

ARTÍCULO 29.- Se clasificará como reservada en los términos del artículo 21, fracción X de la Ley, cuando la información se refiera a la seguridad de las instalaciones estratégicas de los sujetos obligados, y con su difusión se ponga en riesgo de destruir o inhabilitar la infraestructura de carácter indispensable para la provisión de bienes o servicios públicos, vías generales de comunicación, medios de transporte de uso público de jurisdicción estatal o municipal, o servicios de emergencia.

ARTÍCULO 30.- Se considerará información reservada la que, con su difusión menoscabe seriamente el patrimonio de los sujetos obligados, en términos de lo previsto por la fracción XI del artículo 21 de la Ley.

ARTÍCULO 31.- 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.

ARTÍCULO 32.- Se deberá clasificar como reservada, con fundamento en lo dispuesto por la fracción XIII del artículo 21 de la Ley, la información relacionada con la propiedad intelectual, patentes, marcas y procesos industriales, que haya sido recibida por la autoridad bajo la promesa de reserva.

Para los efectos del párrafo anterior, se estará a lo siguiente:

- I. Se clasificará igualmente como reservada la información que señalen las normas especiales con intención de prevenir un posible daño o lesión a los intereses generales o particulares, o bien porque se impida la sana competitividad por contar con información privilegiada de manera anticipada al conocimiento general, entendiéndose éstos: El menoscabo o alteración ne-

gativa del orden público, por provocar como resultado importantes pérdidas o ganancias financieras, pérdida de posiciones competitivas o interferencias en la celebración o ejecución de actos jurídicos de interés público.

II. No se considerará secreto industrial aquella información que sea del dominio público, así como tampoco la que resulte evidente para un técnico en la materia, con base en información previamente disponible, o la que deba ser divulgada por disposición legal o por orden judicial; y

III. No se divulgará ni se considerará del dominio público aquella información que se entregue a un sujeto obligado por parte de la persona que la posea como secreto industrial, cuando la proporcione por disposición legal para el efecto de obtener licencias, permisos, autorizaciones, registros o cualesquier otro documento emitido en plenitud de atribuciones del ente público.

ARTÍCULO 33.- Será reservada la información que organismos internacionales, Estados o municipios entreguen con el carácter de reserva a los sujetos obligados, incluida aquella información que la Federación, organismos internacionales y otros Estados entreguen a los sujetos obligados con carácter de confidencial.

ARTÍCULO 34.- Se considerará información reservada por los sujetos obligados no oficiales, aquella cuya divulgación afecte sus estrategias o funcionamiento interno, así como la 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.

Igualmente, será reservada la información relativa a los procesos deliberativos de los órganos internos de los partidos; la correspondiente a sus estrategias políticas y de campañas electorales; la contenida en todo tipo de encuestas por ellos ordenadas, así como la referida a las actividades de naturaleza privada, personal o familiar de sus afiliados, dirigentes, precandidatos y candidatos a cargos de elección popular.

Será considerada confidencial la información que contenga los datos personales de los afiliados, dirigentes, precandidatos y candidatos a cargos de elección popular, salvo los contenidos en los directorios establecidos en este capítulo y en las listas de precandidatos o candidatos a cargos de elección popular, que solamente contendrán el nombre completo y otros datos personales que autorice el interesado. Se considerará reservada la información relativa a los juicios en curso, de cualquier naturaleza, en que los partidos políticos sean parte, hasta que se encuentren en estado de cosa juzgada.

□ **CAPÍTULO III** DE LA INFORMACIÓN CONFIDENCIAL

ARTÍCULO 35.- 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 íntimo de las víctimas, la explotación de menores o integridad de las personas,
 - d) La información de los partidos políticos que contenga los datos personales de los afiliados, dirigentes, precandidatos y candidatos a cargos de elección popular, salvo los contenidos en los directorios que deberán publicarse de manera oficiosa y en las listas de precandidatos o candidatos a cargos de elección popular, las cuales solamente contendrán el nombre completo y otros datos personales que autorice el interesado; o
 - e) La información de carácter personal incluida 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 realicen 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 36.- Serán datos de carácter personal toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, 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 37.- La información confidencial que los particulares proporcionen a los sujetos obligados para fines estadísticos, así como la que éstos obtengan de registros administrativos u otros que contengan información relativa al estado civil de las personas, no podrá difundirse en forma nominativa o individualizada, ni de cualquier otra manera que permita la identificación inmediata de los interesados, o bien que por su estructura, contenido o grado de desagregación, conduzca a la identificación individual de los mismos.

ARTÍCULO 38.- Con relación a 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 39.- 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 de quienes ostenten la patria potestad del menor o del albacea.

ARTÍCULO 40.- 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 73 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 y de Protección de Datos Personales del Estado de Sonora.

ARTÍCULO 41.- Sin perjuicio de lo que dispongan otras leyes, sólo los interesados o sus representantes podrán solicitar a una unidad de enlace, en las formas ya establecidas y previa acreditación, que les proporcione los datos personales que obren en un sistema de datos personales. En tal caso, 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 la información referida al solicitante.

ARTÍCULO 42.- 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 indiquen las modificaciones por realizarse y se 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 43.- No se considerará confidencial la información que se halle en los registros públicos o en fuentes de acceso público.

ARTÍCULO 44.- 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 45.- 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 46.- 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 47.- 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. La prueba del daño o riesgo que causa 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. Este 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 41 de estos Lineamientos.

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 48.- 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 49.- 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 50.- Tratándose de información clasificada como reservada, el comité de información y/o 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 51.- 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 52.- El formato para señalar la clasificación de documentos que se consideran reservados en todo o en parte, es el siguiente:

- | | |
|--|---|
| <p>I.- “Sello oficial o logotipo de la dependencia o entidad”.</p> | <p>II. - a).- Fecha de clasificación.
 b).- Unidad administrativa.
 c).- Reservada.
 d).- Período de reserva.
 e).- Fundamento legal.
 f).- Ampliación del período de reserva.
 g).- Rúbrica del titular de la unidad administrativa.
 h).- Fecha de desclasificación.
 i).- Rúbrica y cargo del servidor público.</p> |
|--|---|

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 anotará 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 53.- 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 54.- 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.- | <ul style="list-style-type: none"> a).- Fecha de clasificación. b).- Unidad la administrativa. 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).- Partes o secciones reservadas. i).- Rúbrica y cargo del servidor público. |
|-----|--|------|---|

- 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 55.- 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 V 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 54 de los presentes Lineamientos.

ARTÍCULO 56.- El acuerdo para desclasificar la información reservada a que se refiere la fracción II del artículo 16 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 57.- 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 13 de los presentes Lineamientos.

ARTÍCULO 58.- 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 análogos;
 - 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 análogos.

ARTÍCULO 59.- 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 60.- 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 61.- 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 62.- 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 63.- 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 64.- 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 65.- 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 66.- 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 67.- 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 77 de los presentes Lineamientos.

○ SECCIÓN TERCERA DEL TRATAMIENTO CIERTO, ADECUADO, PERTINENTE Y NO EXCESIVO

ARTÍCULO 68.- A efecto de cumplir con el principio de calidad a que se refiere el artículo 63 de estos 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 69.- 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 70.- 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, 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 71.- 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 72.- 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 tal 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 73.- 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.mx), 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 72 de los Lineamientos Generales*

para la Custodia y 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 74.- 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 72 de los presentes Lineamientos.

ARTÍCULO 75.- 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 76.- 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 77.- 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. 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 78.- 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 79.- El Instituto implementará el Directorio Estatal de Sistemas de Datos Personales, mismo que debe ser actualizado de forma semestral.

ARTÍCULO 80.- 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 81.- 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 82.- 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 83.- 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 84.- 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 85.- 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 86.- 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 87.- 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 88.- 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 89.- 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 recomen-

daciones 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 90.- 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 91.- 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 92.- 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 93.- 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 accedidos, reproducidos, alterados o suprimidos sin autorización;
- IX. Aplicar procedimientos para la destrucción de medios de almacenamiento de respaldo obsoletos que contengan datos personales, y la 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 94.- 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 95.- 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.- Se abrogan los anteriores Lineamientos Generales para el Manejo de la Información Restringida y la Protección de Datos Personales en posesión de los sujetos obligados del Estado de Sonora, y se sustituyen por los presentes.

SEGUNDO.- En atención al plazo determinado en el transitorio único de los lineamientos abrogados por los presentes, respecto a las obligaciones derivadas de la sección sexta, denominada “De la seguridad de los datos personales”, se retoma dicha prórroga de tres años puesta en vigor el día 30 de marzo de 2012, para su cumplimiento a partir del día 30 de marzo de 2015.

TERCERO.- Los presentes lineamientos, aprobados por mayoría del Pleno de este Instituto el día 10 de febrero de 2014, entrarán en vigor al día siguiente de su publicación en el Boletín oficial del Gobierno del Estado.

Esta edición del *Compendio Normativo de Acceso a la Información Pública*, se terminó de imprimir en el mes de Febrero de 2014, con un tiraje de 1,000 ejemplares, en Hermosillo, Sonora, México.

