H. Congreso del Estado de Baja California Sur
Oficialía Mayor
Departamento de Apoyo Parlamentario

Nueva Ley BOGE.88 Extraordinario 24-Diciembre-2025

LEY DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DEL ESTADO DE BAJA CALIFORNIA SUR

Ley publicada en el Boletín Oficial del Gobierno del Estado de Baja California Sur el 24 de diciembre de 2025

TEXTO VIGENTE

Al margen un sello con el Escudo del Estado de Baja California Sur, al calce dice: PODER EJECUTIVO.

VÍCTOR MANUEL CASTRO COSÍO, GOBERNADOR DEL ESTADO DE BAJA CALIFORNIA SUR, A SUS HABITANTES HACE SABER:

QUE EL H. CONGRESO DEL ESTADO, SE HA SERVIDO DIRIGIRME EL SIGUIENTE:

DECRETO 3256

El H. CONGRESO DEL ESTADO DE BAJA CALIFORNIA SUR

D E C R E T A:

SE EXPIDE LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DEL ESTADO DE BAJA CALIFORNIA SUR

ARTÍCULO ÚNICO. Se expide la **Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Baja California Sur**, para quedar de la siguiente manera:

TÍTULO PRIMERO
DISPOSICIONES GENERALES

CAPÍTULO ÚNICO
DEL OBJETO DE LA LEY

Artículo 1
La presente Ley es reglamentaria de los artículos 6º, Base A, y 16, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos, así como del apartado B del artículo 13 de la Constitución Política del Estado Libre y Soberano de Baja California Sur, en materia de protección de datos personales en posesión de sujetos obligados. Sus disposiciones son de orden público, interés social y de observancia general en todo el territorio del Estado de Baja California Sur.

Artículo 2
La presente Ley tiene por objeto:

I. Establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales en posesión de sujetos obligados;

II. Precisar las competencias de la Secretaría de la Contraloría y Transparencia Gubernamental y de las demás autoridades competentes en materia de protección de datos personales en posesión de sujetos obligados;

III. Establecer las bases mínimas y condiciones homogéneas que regirán el tratamiento de los datos personales y el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, mediante procedimientos sencillos y expeditos;

IV. Garantizar la observancia de los principios de protección de datos personales previstos en la presente Ley y demás disposiciones que resulten aplicables;

V. Proteger los datos personales en posesión de cualquier autoridad, entidad, órgano y organismo de los poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, fideicomisos y fondos públicos, partidos políticos, y municipios, con la finalidad de regular su debido tratamiento;

VI. Garantizar que toda persona pueda ejercer el derecho a la protección de sus datos personales;

VII. Promover, fomentar y difundir una cultura de protección de datos personales, y

VIII. Establecer los mecanismos para garantizar el cumplimiento y la efectiva aplicación de las medidas de apremio para aquellas conductas que contravengan lo previsto en esta Ley.

Artículo 3. Para efectos de esta Ley, se entenderá por:

I. **Áreas:** Instancias de los sujetos obligados previstas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes, que cuenten o puedan contar, dar tratamiento y ser responsables o encargadas de los datos personales;

II. **Autoridades garantes:** La Contraloría del Poder Judicial del Estado; los órganos internos de control o equivalentes de los órganos constitucionales autónomos; la Contraloría del Poder Legislativo; y el Instituto Estatal Electoral, por cuanto hace al acceso a la protección de datos personales a cargo de los partidos políticos;

III. **Aviso de privacidad:** Documento a disposición de la persona titular de la información, de forma física, electrónica o en cualquier otro formato, generado por el responsable desde el momento en que se recaben sus datos personales, con el objeto de informarle los propósitos de su tratamiento;

IV. **Bases de datos:** Conjunto ordenado de datos personales referentes a una persona identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización;

V. **Bloqueo:** Identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y, transcurrido éste, se procederá a su cancelación en la base de datos que corresponda;

VI. **Comité de Transparencia:** Instancia a la que hace referencia el artículo 39 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Baja California Sur;

VII. **Cómputo en la nube:** Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente;

VIII. **Consentimiento:** Manifestación de la voluntad libre, específica e informada de la persona titular de los datos, mediante la cual se efectúa su tratamiento;

IX. **Datos personales:** Cualquier información concerniente a una persona identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información;

X. **Datos personales sensibles:** Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para ésta. De manera enunciativa más no limitativa, se consideran sensibles los datos que revelen origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;

XI. **Derechos ARCO:** Derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales;

XII. **Días:** Días hábiles;

XIII. **Disociación:** Procedimiento mediante el cual los datos personales no pueden asociarse a la persona titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación de la misma;

XIV. Documento de seguridad: Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee;

XV. Evaluación de impacto en la protección de datos personales: Documento mediante el cual los sujetos obligados que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, valoran los impactos reales respecto de determinado tratamiento, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de las personas titulares, así como los deberes de los responsables y las personas encargadas, previstos en las disposiciones jurídicas aplicables;

XVI. Fuentes de acceso público: Aquellas bases de datos, sistemas o archivos que por disposición de ley puedan ser consultadas públicamente cuando no exista impedimento por una norma limitativa y sin más exigencia que, en su caso, el pago de una contraprestación, tarifa o contribución. No se considerará fuente de acceso público cuando la información contenida en la misma sea obtenida o tenga una procedencia ilícita;

XVII. Medidas compensatorias: Mecanismos alternos para dar a conocer a las personas titulares el aviso de privacidad, a través de su difusión por medios masivos de comunicación u otros de amplio alcance;

XVIII. Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales;

XIX. Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal en materia de protección de datos personales;

XX. Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento, tales como:

a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;

b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;

c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y

d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad;

XXI. Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y de los recursos involucrados en su tratamiento, tales como:

a) Prevenir que el acceso a las bases de datos o a la información sea por usuarios identificados y autorizados;

b) Generar un esquema de privilegios para que el usuario lleve a cabo únicamente las actividades necesarias para el cumplimiento de sus funciones;

c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y

d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales;

XXII. Persona encargada: Persona física o jurídica, pública o privada, ajena a la organización de la persona responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta de la persona responsable;

XXIII. Persona titular: Sujeto a quien corresponden los datos personales;

XXIV. Plataforma Nacional: La Plataforma Nacional de Transparencia a que hace referencia el artículo 44 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Baja California Sur;

XXV. Remisión: Toda comunicación de datos personales realizada exclusivamente entre el responsable y la persona encargada, dentro o fuera del territorio mexicano;

XXVI. Responsable: Sujetos obligados a que se refiere la fracción XXVII del presente artículo que deciden sobre el tratamiento de datos personales;

XXVII. Secretaría: La Secretaría de la Contraloría y Transparencia Gubernamental;

XXVIII. Sujetos obligados: Cualquier autoridad, entidad, órgano y organismo de los poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, en el ámbito estatal y municipal;

XXIX. Supresión: Baja archivística de los datos personales conforme a las disposiciones jurídicas aplicables en materia de archivos, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable;

XXX. Transferencia: Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta de la titular, del responsable o de la persona encargada;

XXXI. Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales; y

XXXII. Unidad de Transparencia: Instancia a la que hace referencia el artículo 41 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Baja California Sur.

Artículo 4
La presente Ley será aplicable a cualquier tratamiento de datos personales que obren en soportes físicos, electrónicos o en cualquier otro formato, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Artículo 5
Para efectos de esta Ley, se considerarán como fuentes de acceso público:

I. Las páginas de Internet o medios remotos o locales de comunicación electrónica, óptica u otra tecnología, siempre que el sitio donde se encuentren los datos personales esté concebido para facilitar información al público y abierto a la consulta general;

II. Los directorios telefónicos en términos de la normativa aplicable;

III. Los diarios, gacetas o boletines oficiales, de acuerdo con las disposiciones jurídicas correspondientes;

IV. Los medios de comunicación social, y

V. Los registros públicos conforme a las disposiciones que les resulten aplicables.

Para que los supuestos enumerados en este artículo sean considerados fuentes de acceso público será necesario que su consulta pueda ser realizada por cualquier

persona no impedida por una norma limitativa, o sin más exigencia que, en su caso, el pago de una contraprestación, derecho o tarifa.

No se considerará fuente de acceso público cuando la información contenida sea obtenida o tenga una procedencia ilícita.

Artículo 6
El Estado garantizará la privacidad de los individuos y deberá velar porque terceras personas no incurran en conductas que puedan afectarla arbitrariamente.

El derecho a la protección de los datos personales solamente podrá limitarse por razones de seguridad nacional, en términos de la ley aplicable, por disposiciones de orden público, seguridad y salud públicas, o para proteger los derechos de terceros.

Artículo 7
Por regla general no podrán tratarse datos personales sensibles, salvo que se cuente con el consentimiento expreso de la persona titular o, en su defecto, se actualicen los supuestos previstos en el artículo 16 de esta Ley.

En el tratamiento de datos personales de niñas, niños y adolescentes deberá privilegiarse en todo momento el interés superior de la niñez, conforme a las disposiciones jurídicas aplicables.

Artículo 8
La aplicación e interpretación de esta Ley se realizará conforme a lo dispuesto en la Constitución Política de los Estados Unidos Mexicanos, los tratados internacionales de los que el Estado mexicano sea parte, la Constitución Política del Estado Libre y Soberano de Baja California Sur, así como las resoluciones y sentencias vinculantes que emitan los órganos jurisdiccionales nacionales e internacionales especializados.

En todo tiempo deberá favorecerse la protección más amplia a la privacidad y a los derechos de las personas en materia de protección de datos personales.

Para efectos de interpretación, se podrán tomar en cuenta los criterios, determinaciones y opiniones de los organismos nacionales e internacionales especializados en la materia.

Artículo 9
A falta de disposición expresa en esta Ley, se aplicarán de manera supletoria las disposiciones del Código de Procedimientos Civiles para el Estado de Baja California Sur y de la Ley de Procedimiento Administrativo del Estado de Baja California Sur.

TÍTULO SEGUNDO
PRINCIPIOS Y DEBERES

CAPÍTULO PRIMERO
DE LOS PRINCIPIOS

Artículo 10
El responsable deberá observar en todo tratamiento de datos personales los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad.

Artículo 11
El tratamiento de datos personales por parte del responsable deberá sujetarse a las facultades y atribuciones que la normatividad aplicable le confiera.

Artículo 12
Todo tratamiento de datos personales deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones legales del responsable.

El responsable podrá tratar datos personales para finalidades distintas a las establecidas en el aviso de privacidad, siempre que cuente con atribuciones conferidas en la legislación aplicable y medie el consentimiento de la persona titular, salvo en los supuestos previstos en esta Ley o en la legislación aplicable en la materia.

Artículo 13
El responsable no deberá obtener ni tratar datos personales mediante medios engañosos o fraudulentos y deberá privilegiar la protección de los intereses de la persona titular y la expectativa razonable de privacidad.

Artículo 14
Cuando no se actualicen las causales de excepción previstas en el artículo 16 de esta Ley, el responsable deberá contar con el consentimiento previo de la persona titular para el tratamiento de los datos personales, el cual deberá otorgarse de forma:

a) **Libre:** Sin que medie error, mala fe, violencia o dolo que afecten la manifestación de voluntad de la persona titular;

b) **Específica:** Referida a finalidades concretas, lícitas, explícitas y legítimas que justifiquen el tratamiento, y

c) **Informada:** Que la persona titular conozca el aviso de privacidad previo al tratamiento a que serán sometidos sus datos personales.

En el caso de personas menores de edad o que se encuentren en estado de interdicción o incapacidad declarada, se estará a lo dispuesto en la legislación civil aplicable.

Artículo 15

El consentimiento podrá manifestarse de forma expresa o tácita.

Se entenderá que el consentimiento es expreso cuando la voluntad de la persona titular se manifieste verbalmente, por escrito, por medios electrónicos, ópticos, signos inequívocos o cualquier otra tecnología.

Será tácito cuando, habiéndose puesto a disposición de la persona titular el aviso de privacidad, ésta no manifieste su oposición.

Por regla general, será válido el consentimiento tácito, salvo cuando la normativa aplicable exija que la voluntad se manifieste expresamente.

Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito de la persona titular, mediante firma autógrafa, firma electrónica o cualquier mecanismo de autenticación aplicable, salvo en los casos previstos en el artículo 16 de esta Ley.

Artículo 16
El responsable no estará obligado a recabar el consentimiento de la persona titular para el tratamiento de sus datos personales en los siguientes casos:

I. Cuando la legislación aplicable así lo disponga, debiendo dichos supuestos ser acordes con los principios establecidos en esta Ley;

II. Cuando las transferencias entre responsables se realicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento;

III. Cuando exista orden judicial, resolución o mandato fundado y motivado de autoridad competente;

IV. Para el reconocimiento, ejercicio o defensa de derechos de la persona titular ante autoridad competente;

V. Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre la persona titular y el responsable;

VI. Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o bienes;

VII. Cuando los datos sean necesarios para la prevención, diagnóstico o la prestación de asistencia sanitaria;

VIII. Cuando los datos personales figuren en fuentes de acceso público;

IX. Cuando los datos personales se sometan a un procedimiento previo de disociación, o

X. En los supuestos previstos en la legislación aplicable en materia de seguridad y procuración de justicia.

Artículo 17
El responsable deberá adoptar medidas para mantener exactos, completos, correctos y actualizados los datos personales en su posesión.

Se presume la calidad de los datos cuando éstos son proporcionados directamente por la persona titular, salvo prueba en contrario.

Cuando los datos hayan dejado de ser necesarios para las finalidades previstas en el aviso de privacidad, deberán ser suprimidos previo bloqueo, una vez concluido el plazo de conservación correspondiente.

Artículo 18
El responsable deberá establecer y documentar procedimientos para la conservación, bloqueo y supresión de los datos personales, en los cuales se incluyan los periodos de conservación conforme a las disposiciones aplicables.

Dichos procedimientos deberán prever mecanismos de revisión periódica sobre la necesidad de conservar los datos personales.

Artículo 19
El responsable sólo podrá tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.

Artículo 20
El responsable deberá informar a la persona titular, mediante el aviso de privacidad, la existencia y características principales del tratamiento de sus datos personales, a fin de que pueda tomar decisiones informadas.

El aviso de privacidad deberá estar redactado de forma clara y sencilla, y ponerse a disposición de la persona titular en sus modalidades integral y simplificada.

Artículo 21
El aviso de privacidad integral deberá contener, al menos:

I. La denominación y domicilio del responsable;

II. Los datos personales que serán sometidos a tratamiento, identificando aquéllos que son sensibles;

III. El fundamento legal que faculta al responsable para llevar a cabo el tratamiento;

IV. Las finalidades del tratamiento, distinguiendo aquellas que requieran consentimiento de la persona titular;

V. Los mecanismos y medios disponibles para ejercer los derechos ARCO;

VI. El domicilio de la Unidad de Transparencia;

VII. Cuando se realicen transferencias que requieran consentimiento:

a) Las autoridades, entidades, órganos y organismos a los que se transfieran los datos personales; y

b) Las finalidades de dichas transferencias;

VIII. Los mecanismos disponibles para que la persona titular pueda manifestar su negativa al tratamiento o transferencia de datos personales que requieran su consentimiento, y

IX. Los medios por los cuales el responsable comunicará los cambios al aviso de privacidad.

Artículo 22
El aviso de privacidad en su modalidad simplificada deberá contener, al menos, la información señalada en las fracciones I, IV, VII y VIII del artículo anterior, y el sitio donde pueda consultarse el aviso integral.

La puesta a disposición del aviso simplificado no exime al responsable de permitir el acceso al aviso integral.

Artículo 23
El responsable deberá implementar mecanismos para acreditar el cumplimiento de los principios, deberes y obligaciones previstos en esta Ley y rendir cuentas sobre el tratamiento de datos personales en su posesión, ante la persona titular, la Secretaría o las autoridades garantes, según corresponda.

En la implementación de estos mecanismos se podrá recurrir a estándares o mejores prácticas nacionales e internacionales, siempre que no contravengan la legislación aplicable.

Artículo 24
Para dar cumplimiento al principio de responsabilidad, el responsable deberá, al menos:

I. Destinar los recursos autorizados para implementar programas y políticas de protección de datos personales;

II. Elaborar políticas y programas internos obligatorios en materia de protección de datos personales;

III. Capacitar y actualizar periódicamente al personal en esta materia;

IV. Revisar periódicamente las políticas y programas de seguridad de datos personales;

V. Establecer mecanismos de supervisión y auditoría interna o externa para verificar el cumplimiento de dichas políticas;

VI. Establecer procedimientos para recibir y atender dudas y quejas de las personas titulares;

VII. Diseñar e implementar políticas públicas, programas, servicios y sistemas que impliquen tratamiento de datos personales, conforme a esta Ley; y

VIII. Garantizar que los programas y sistemas que impliquen tratamiento de datos personales cumplan por defecto con las obligaciones previstas en esta Ley y demás disposiciones aplicables.

CAPÍTULO SEGUNDO
DE LOS DEBERES

Artículo 25
Con independencia del sistema en que se encuentren los datos personales o el tipo de tratamiento que se realice, el responsable deberá establecer y mantener medidas de seguridad administrativas, físicas y técnicas que garanticen la confidencialidad, integridad, disponibilidad y protección de los datos personales contra daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado.

Artículo 26
Las medidas de seguridad adoptadas deberán considerar, al menos:

I. El riesgo inherente a los datos personales tratados;

II. La sensibilidad de los datos personales;

III. El desarrollo tecnológico aplicable;

IV. Las posibles consecuencias de una vulneración para las personas titulares;

V. Las transferencias de datos personales que se realicen;

VI. El número de personas titulares;

VII. Las vulneraciones previas ocurridas, y

VIII. El riesgo derivado del valor potencial que pudieran tener los datos personales tratados para un tercero no autorizado.

Artículo 27
Para establecer y mantener las medidas de seguridad, el responsable deberá realizar, al menos, las siguientes actividades:

I. Crear políticas internas de gestión y tratamiento de datos personales que consideren el ciclo de vida de éstos;

II. Definir funciones y obligaciones del personal que intervenga en el tratamiento;

III. Elaborar un inventario de datos personales y de los sistemas de tratamiento;

IV. Realizar un análisis de riesgos, identificando amenazas y vulnerabilidades;

V. Realizar un análisis de brechas, comparando medidas existentes contra las faltantes;

VI. Elaborar un plan de trabajo para implementar y mantener las medidas de seguridad;

VII. Monitorear y revisar periódicamente las medidas de seguridad adoptadas, y

VIII. Capacitar al personal conforme a sus roles y responsabilidades.

Artículo 28
Las acciones relacionadas con la seguridad deberán documentarse e integrarse en un sistema de gestión que permita establecer, implementar, monitorear, revisar y mejorar las medidas adoptadas.

Artículo 29
El responsable deberá elaborar un documento de seguridad que contenga, al menos:

I. El inventario de datos personales y de sistemas de tratamiento;

II. Funciones y obligaciones del personal autorizado;

III. El análisis de riesgos;

IV. El análisis de brechas;

V. El plan de trabajo;

VI. Mecanismos de monitoreo y revisión, y

VII. El programa general de capacitación.

Artículo 30
El documento de seguridad deberá actualizarse cuando:

I. Se modifique sustancialmente el tratamiento de datos personales y ello altere el nivel de riesgo;

II. Como resultado de un proceso de mejora continua;

III. Como consecuencia de vulneraciones de seguridad, o

IV. Se implementen acciones correctivas y preventivas derivadas de incidentes.

Artículo 31
En caso de vulneración a la seguridad, el responsable deberá analizar las causas e implementar acciones preventivas y correctivas en su plan de trabajo, a fin de evitar su repetición.

Artículo 32
Se considerarán vulneraciones de seguridad, entre otras:

I. La pérdida o destrucción no autorizada;

II. El robo, extravío o copia indebida;

III. El uso, acceso o tratamiento no autorizado, y

IV. El daño, alteración o modificación indebida.

Artículo 33
El responsable deberá llevar una bitácora de vulneraciones a la seguridad, que describa el incidente, la fecha de ocurrencia, el motivo y las acciones correctivas implementadas.

Artículo 34
El responsable deberá informar, sin dilación, a la persona titular y, en su caso, a la Secretaría y a las Autoridades garantes, sobre las vulneraciones que afecten de manera significativa los derechos patrimoniales o morales, una vez confirmada la vulneración e iniciadas las acciones de atención correspondientes.

Artículo 35
El responsable deberá comunicar a la persona titular, al menos:

I. La naturaleza del incidente;

II. Los datos personales comprometidos;

III. Recomendaciones para proteger sus intereses;

IV. Las acciones correctivas inmediatas, y

V. Los medios para obtener mayor información.

Artículo 36
El responsable deberá establecer controles que aseguren que todas las personas que intervengan en cualquier fase del tratamiento de los datos personales guarden confidencialidad respecto de éstos, obligación que subsistirá aún después de concluir su relación con el responsable.

Lo anterior, sin perjuicio de lo dispuesto en la normativa de acceso a la información pública.

TÍTULO TERCERO
DERECHOS DE LAS PERSONAS TITULARES Y SU EJERCICIO

CAPÍTULO PRIMERO
DE LOS DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN

Artículo 37
La persona titular o su representante podrán solicitar al responsable, en cualquier momento, el acceso, rectificación, cancelación u oposición al tratamiento de sus datos personales (derechos ARCO). El ejercicio de un derecho no condiciona ni limita el ejercicio de los demás.

Artículo 38
La persona titular tiene derecho a acceder a sus datos personales que obren en posesión del responsable, así como a conocer las condiciones y generalidades de su tratamiento.

Artículo 39
La persona titular tiene derecho a solicitar la rectificación de sus datos personales cuando éstos resulten inexactos, incompletos o desactualizados.

Artículo 40
La persona titular tiene derecho a solicitar la cancelación de sus datos personales de archivos, registros, expedientes y sistemas del responsable, a fin de que dejen de estar en su posesión y de ser tratados.

Artículo 41
La persona titular podrá oponerse al tratamiento de sus datos personales o exigir que cese, cuando:

I. Aun siendo lícito el tratamiento, su persistencia pueda causarle daño o perjuicio; y

II. Sus datos personales sean objeto de tratamiento automatizado que produzca efectos jurídicos no deseados o afecte de manera significativa sus derechos o libertades, sin intervención humana.

CAPÍTULO SEGUNDO
DEL EJERCICIO DE LOS DERECHOS ARCO

Artículo 42
La recepción y trámite de solicitudes para el ejercicio de derechos ARCO se sujetará al procedimiento previsto en este Título y demás disposiciones aplicables.

Artículo 43
Para ejercer derechos ARCO se deberá acreditar la identidad de la persona titular y, en su caso, la representación legal.

El ejercicio de derechos por persona distinta a la titular sólo será posible en los supuestos previstos por la ley o por mandato judicial.

En el caso de menores de edad o personas en estado de interdicción, se estará a lo previsto en la legislación civil aplicable.

Tratándose de datos de personas fallecidas, podrá ejercer derechos quien acredite interés jurídico, siempre que la persona titular lo hubiera autorizado o exista mandato judicial.

Artículo 44
El ejercicio de los derechos ARCO es gratuito. Sólo podrán cobrarse costos de reproducción, certificación o envío, en términos de la normatividad aplicable.

La información deberá entregarse sin costo cuando no exceda de veinte hojas simples.

No podrá establecerse servicio o medio que implique un costo adicional para la presentación de solicitudes.

Artículo 45
El responsable deberá establecer procedimientos sencillos para el ejercicio de derechos ARCO.

El plazo de respuesta no podrá exceder de veinte días hábiles contados a partir del día siguiente de la recepción de la solicitud. Dicho plazo podrá ampliarse por una sola ocasión hasta por diez días, cuando existan circunstancias que lo justifiquen y se notifique a la persona titular.

Si resulta procedente, el responsable hará efectivo el derecho en un plazo que no podrá exceder de quince días hábiles contados a partir de la notificación de la respuesta.

Artículo 46
La solicitud deberá contener, al menos:

I. Nombre y domicilio o medio para recibir notificaciones;

II. Documentos que acrediten identidad o representación legal;

III. Área responsable que trata los datos, de ser posible;

IV. Descripción clara de los datos personales respecto de los que se pretende ejercer algún derecho, salvo en el caso del derecho de acceso;

V. Descripción del derecho ARCO que se pretende ejercer, y

VI. Cualquier otro elemento que facilite la localización de los datos.

Tratándose de solicitudes de acceso, la persona titular deberá señalar la modalidad de entrega preferida. El responsable deberá atender dicha preferencia, salvo imposibilidad física o jurídica, caso en el cual deberá ofrecer una alternativa fundada y motivada.

En caso de solicitudes incompletas, se prevendrá al solicitante dentro de los cinco días siguientes para que subsane en un plazo de diez días. La falta de subsanación implicará que la solicitud se tenga por no presentada.

Artículo 47
Cuando el responsable no sea competente para atender la solicitud, deberá informarlo a la persona titular dentro de los tres días siguientes y, en su caso, orientarla hacia el responsable competente.

Si se declara inexistencia de los datos personales, esta circunstancia deberá constar en resolución del Comité de Transparencia.

Artículo 48
Cuando exista un procedimiento específico en disposiciones aplicables para el ejercicio de derechos ARCO, el responsable deberá informar de su existencia a la persona titular en un plazo no mayor a cinco días, para que ésta decida el trámite a seguir.

Artículo 49
El ejercicio de los derechos ARCO no será procedente cuando:

I. No se acredite identidad o representación legal;

II. Los datos personales no obren en posesión del responsable;

III. Exista impedimento legal;

IV. Se lesionen derechos de un tercero;

V. Se obstaculicen actuaciones judiciales o administrativas;

VI. Exista resolución de autoridad competente que restrinja el acceso, rectificación, cancelación u oposición;

VII. La cancelación u oposición haya sido previamente realizada;

VIII. El responsable no sea competente;

IX. Los datos sean necesarios para proteger intereses jurídicamente tutelados de la persona titular;

X. Sean necesarios para cumplir obligaciones legalmente adquiridas;

XI. En ejercicio de atribuciones legales, su resguardo y uso resulten necesarios y proporcionales para mantener la integridad y estabilidad del Estado mexicano; o

XII. Los datos formen parte de información entregada por entidades sujetas a regulación y supervisión financiera, conforme a requerimientos legales.

En todos los casos, el responsable deberá informar a la persona titular el motivo de la negativa, en el plazo previsto en el artículo 45.

Artículo 50
Contra la negativa de trámite o falta de respuesta del responsable procederá el recurso de revisión previsto en esta Ley.

CAPÍTULO TERCERO
DE LA PORTABILIDAD DE LOS DATOS

Artículo 51
Cuando los datos personales sean tratados electrónicamente en un formato estructurado y comúnmente utilizado, la persona titular tendrá derecho a obtener una copia de los mismos en dicho formato.

Cuando el tratamiento se base en el consentimiento o en un contrato, la persona titular podrá transmitir sus datos personales a otro responsable, sin impedimentos por parte del responsable original.

TÍTULO CUARTO
RELACIÓN DEL RESPONSABLE Y LA PERSONA ENCARGADA

CAPÍTULO ÚNICO
RESPONSABLE Y PERSONA ENCARGADA

Artículo 52
La persona encargada realizará el tratamiento de datos personales únicamente conforme a las instrucciones del responsable, sin ostentar facultades de decisión sobre el alcance o contenido del mismo.

Artículo 53
La relación entre responsable y persona encargada deberá formalizarse mediante contrato o instrumento jurídico que permita acreditar su existencia, alcance y contenido, el cual deberá contener, al menos, las siguientes cláusulas:

I. Realizar el tratamiento conforme a las instrucciones del responsable;

II. Abstenerse de tratar los datos para finalidades distintas a las instruidas;

III. Implementar las medidas de seguridad aplicables;

IV. Informar al responsable sobre vulneraciones de seguridad;

V. Guardar confidencialidad respecto de los datos tratados;

VI. Suprimir o devolver los datos una vez cumplida la relación jurídica, salvo disposición legal en contrario, y

VII. Abstenerse de transferir datos salvo instrucción del responsable;

VIII. Dar toda la información requerida por la Secretaria o la Autoridad Garante, sobre el tratamiento que se les da a los datos personales.

Artículo 54
Si la persona encargada incumple las instrucciones del responsable o con el debido tratamiento de los datos personales de conformidad con esta legislación, asumirá el carácter de responsable y las consecuencias legales correspondientes.

Artículo 55

El procedimiento de contratación de la persona encargada deberá seguir las reglas establecidas en la Ley de Adquisiciones, Arrendamientos y Servicios del Estado de Baja California Sur.

Artículo 56
La persona encargada deberá responder todas las solicitudes de información, en el tiempo que le solicite la Secretaria o la Autoridad Garante.

Artículo 57
El responsable podrá contratar servicios, aplicaciones o infraestructura en cómputo en la nube, siempre que la persona proveedora garantice políticas de protección de datos equivalentes a los principios y deberes establecidos en esta Ley.

Artículo 58
Para adherirse a servicios de cómputo en la nube bajo condiciones generales de contratación, el responsable sólo podrá utilizar aquellos que:

I. Cuenten con políticas de protección de datos personales que:

a) Sean afines a los principios de esta Ley;

b) Transparenten las subcontrataciones involucradas;

c) Se abstengan de asumir la titularidad o propiedad de la información, y

d) Garanticen confidencialidad.

II. Dispongan de mecanismos que permitan:

a) Informar sobre cambios en políticas de privacidad o condiciones del servicio;

b) Permitir al responsable limitar el tratamiento de los datos;

c) Mantener medidas de seguridad adecuadas;

d) Garantizar la supresión de datos al término del servicio, y

e) Restringir el acceso a personas no autorizadas, informando al responsable en caso de requerimiento fundado de autoridad competente.

En ningún caso podrá contratarse un servicio que no garantice la debida protección de los datos personales.

TÍTULO QUINTO
COMUNICACIONES DE DATOS PERSONALES

CAPÍTULO ÚNICO
DE LAS TRANSFERENCIAS Y REMISIONES DE DATOS PERSONALES

Artículo 59
Toda transferencia de datos personales, nacional o internacional, requiere el consentimiento de la persona titular, salvo las excepciones previstas en esta Ley.

Artículo 60
La transferencia deberá formalizarse mediante cláusulas contractuales, convenios o instrumentos jurídicos que acrediten su alcance y las obligaciones de las partes, salvo en los siguientes casos:

I. Transferencias nacionales entre responsables en cumplimiento de disposición legal o ejercicio de atribuciones conferidas, y

II. Transferencias internacionales previstas en ley, tratado suscrito por México, o realizadas a petición de autoridad extranjera u organismo internacional competente, siempre que exista equivalencia de atribuciones o finalidad.

Artículo 61
En las transferencias nacionales, el receptor deberá comprometerse a garantizar la confidencialidad de los datos y utilizarlos únicamente para los fines que motivaron su transmisión.

Artículo 62
El responsable sólo podrá transferir datos fuera del territorio nacional cuando el receptor se obligue a protegerlos conforme a los principios establecidos en esta Ley.

Artículo 63
En toda transferencia, el responsable deberá comunicar al receptor el aviso de privacidad aplicable.

Artículo 64
No se requerirá consentimiento de la persona titular en los siguientes supuestos:

I. Cuando la transferencia esté prevista en esta u otras leyes o en tratados internacionales;

II. Cuando se realice entre responsables para el ejercicio de facultades propias, compatibles o análogas;

III. Para la investigación y persecución de delitos, procuración o administración de justicia;

IV. Para el reconocimiento, ejercicio o defensa de un derecho ante autoridad competente;

V. Para la prevención, diagnóstico o prestación de asistencia sanitaria, tratamiento o gestión de servicios de salud;

VI. Para el cumplimiento o mantenimiento de una relación jurídica entre responsable y titular;

VII. Cuando sea necesaria por virtud de contrato en interés de la persona titular;

VIII. Cuando se actualicen los supuestos del artículo 16 de esta Ley, o

IX. Por razones de seguridad nacional.

Artículo 65
Las remisiones nacionales e internacionales de datos personales entre el responsable y la persona encargada no requerirán ser informadas a la persona titular ni contar con su consentimiento.

TÍTULO SEXTO
ACCIONES PREVENTIVAS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

CAPÍTULO PRIMERO
DE LAS MEJORES PRÁCTICAS

Artículo 66
Para el cumplimiento de esta Ley, el responsable podrá adoptar, individualmente o en colaboración con otros responsables, encargados u organizaciones, esquemas de mejores prácticas con los objetivos de:

I. Elevar el nivel de protección de los datos personales;

II. Armonizar tratamientos en sectores específicos;

III. Facilitar el ejercicio de los derechos ARCO;

IV. Facilitar transferencias entre responsables;

V. Complementar la normatividad aplicable, y

VI. Demostrar ante la Secretaría o las Autoridades garantes el cumplimiento de las obligaciones en la materia.

Artículo 67
Los esquemas que busquen validación o reconocimiento deberán:

I. Cumplir los criterios y parámetros que emita la Secretaría o la Autoridad garante competente, y

II. Notificarse conforme al procedimiento previsto por dichas autoridades para su evaluación, y, en su caso, validación o reconocimiento e inscripción en el registro correspondiente.

La Secretaría y las Autoridades garantes, según su competencia, emitirán reglas de operación de los registros e inscribirán los esquemas validados o reconocidos.

Artículo 68
Cuando el responsable pretenda poner en operación o modificar políticas públicas, sistemas, plataformas o tecnologías que impliquen tratamiento intensivo o relevante de datos personales, deberá elaborar una evaluación de impacto en protección de datos personales y presentarla a la Secretaría o a la Autoridad garante competente, las cuales podrán emitir recomendaciones no vinculantes.

El contenido mínimo de la evaluación será determinado por la autoridad competente.

Artículo 69
Se considerará tratamiento intensivo o relevante cuando:

I. Existan riesgos inherentes elevados a los datos por tratar;

II. Se traten datos personales sensibles, o

III. Se efectúen o pretendan efectuar transferencias de datos personales.

Artículo 70
La Secretaría o la Autoridad garante, con base en parámetros objetivos, podrá emitir criterios adicionales para determinar tratamientos intensivos o relevantes, considerando:

I. Número de personas titulares involucradas;

II. Público objetivo;

III. Desarrollo tecnológico utilizado, y

IV. Impacto social o económico, o interés público del tratamiento.

Artículo 71
La evaluación de impacto deberá presentarse con al menos treinta días naturales de anticipación a la fecha prevista para la operación o modificación del tratamiento, para la emisión, en su caso, de recomendaciones.

Artículo 72
La Secretaría o la Autoridad garante, según corresponda, podrá emitir recomendaciones no vinculantes dentro de los treinta días naturales siguientes a la presentación de la evaluación.

Artículo 73
Excepcionalmente, cuando la publicidad de la evaluación comprometa los efectos del programa o existan situaciones de emergencia o urgencia, el responsable podrá prescindir de la evaluación de impacto, dejando constancia fundada y motivada y adoptando medidas reforzadas de seguridad.

CAPÍTULO SEGUNDO
DE LAS BASES DE DATOS EN INSTANCIAS DE SEGURIDAD, PROCURACIÓN Y ADMINISTRACIÓN DE JUSTICIA

Artículo 74
La obtención y tratamiento de datos personales por sujetos obligados competentes en seguridad, procuración y administración de justicia se limitará a supuestos necesarios y proporcionales para el ejercicio de sus funciones en seguridad nacional, seguridad pública, prevención o persecución de delitos, debiendo almacenarse en bases de datos específicas.

Artículo 75
En dichos tratamientos deberán observarse los principios del Título Segundo. Las comunicaciones privadas son inviolables; sólo la autoridad judicial competente, a petición de autoridad facultada por la ley, podrá autorizar su intervención.

Artículo 76
Los responsables de estas bases deberán establecer medidas de seguridad de nivel alto para garantizar integridad, disponibilidad y confidencialidad, y prevenir daño, pérdida, alteración, destrucción, uso, acceso o tratamiento no autorizados.

TÍTULO SÉPTIMO
RESPONSABLES EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS SUJETOS OBLIGADOS

CAPÍTULO PRIMERO
COMITÉ DE TRANSPARENCIA

Artículo 77
Cada responsable contará con un Comité de Transparencia, que se integrará y funcionará conforme a la Ley de Transparencia y Acceso a la Información Pública del Estado de Baja California Sur y demás disposiciones aplicables. El Comité será la máxima instancia del responsable en materia de protección de datos personales.

Artículo 78
Sin perjuicio de otras atribuciones, el Comité tendrá, al menos, las siguientes funciones:

I. Coordinar y supervisar acciones para garantizar el derecho a la protección de datos personales en la organización;

II. Instituir, en su caso, procedimientos internos para la gestión eficiente de solicitudes ARCO;

III. Confirmar, modificar o revocar determinaciones de inexistencia de datos personales o negativas al ejercicio de derechos ARCO;

IV. Establecer y supervisar criterios específicos para la mejor observancia de esta Ley;

V. Supervisar, con las áreas competentes, el cumplimiento de medidas y controles del documento de seguridad;

VI. Dar seguimiento y cumplimiento a resoluciones de la Secretaría o de las Autoridades garantes;

VII. Establecer programas de capacitación y actualización para personas servidoras públicas; y

VIII. Dar vista al órgano interno de control o instancia equivalente cuando advierta presuntas irregularidades en tratamientos de datos, en especial en casos de inexistencia declarada.

CAPÍTULO SEGUNDO
DE LA UNIDAD DE TRANSPARENCIA

Artículo 79
Cada responsable contará con una Unidad de Transparencia, que se integrará y funcionará conforme a la Ley de Transparencia estatal y tendrá, además, las funciones de:

I. Auxiliar y orientar a las personas titulares sobre el ejercicio del derecho a la protección de datos personales;

II. Gestionar las solicitudes ARCO;

III. Establecer mecanismos para asegurar que los datos sólo se entreguen a la persona titular o su representante acreditado;

IV. Informar los costos de reproducción y envío conforme a la normatividad aplicable;

V. Proponer al Comité procedimientos internos que fortalezcan la gestión de solicitudes ARCO;

VI. Aplicar instrumentos de evaluación de calidad sobre la gestión de solicitudes ARCO; y

VII. Asesorar a las áreas del responsable en materia de protección de datos personales.

Los responsables que, por sus funciones, realicen tratamientos intensivos o relevantes podrán designar un oficial de protección de datos personales, quien integrará la Unidad y realizará las atribuciones anteriores.

Los sujetos obligados promoverán acuerdos de accesibilidad con instituciones públicas especializadas para recepción, trámite y entrega de respuestas en lenguas indígenas, braille u otros formatos accesibles.

Artículo 80
El responsable procurará que las personas con discapacidad y grupos de atención prioritaria puedan ejercer, en igualdad de circunstancias, su derecho a la protección de datos personales.

TÍTULO OCTAVO
AUTORIDADES GARANTES

CAPÍTULO PRIMERO
DE LA SECRETARÍA

Artículo 81
La Secretaría tendrá las siguientes atribuciones:

I. Garantizar el ejercicio del derecho a la protección de datos personales en posesión de sujetos obligados;

II. Interpretar administrativamente la presente Ley;

III. Conocer y resolver los recursos de revisión interpuestos por personas titulares;

IV. Conocer y resolver, de oficio o a petición fundada de las Autoridades garantes, los recursos de revisión que por su interés y trascendencia lo ameriten;

V. Conocer, sustanciar y resolver los procedimientos de verificación;

VI. Establecer y ejecutar las medidas de apremio previstas en esta Ley;

VII. Denunciar ante autoridades competentes las presuntas infracciones a la Ley y aportar pruebas;

VIII. Coordinarse con autoridades para garantizar que las solicitudes ARCO y recursos de revisión en lenguas indígenas sean atendidos en la misma lengua;

IX. Garantizar condiciones de accesibilidad para personas y grupos de atención prioritaria;

X. Elaborar y publicar estudios e investigaciones en la materia;

XI. Proporcionar apoyo técnico a los responsables;

XII. Divulgar y emitir recomendaciones, estándares y mejores prácticas;

XIII. Vigilar y verificar el cumplimiento de la Ley;

XIV. Administrar el registro de esquemas de mejores prácticas y emitir sus reglas de operación;

XV. Emitir recomendaciones no vinculantes sobre evaluaciones de impacto;

XVI. Expedir disposiciones generales sobre el procedimiento de verificación;

XVII. Evaluar los esquemas de mejores prácticas notificados y resolver sobre su validación, reconocimiento e inscripción en el registro;

XVIII. Emitir disposiciones administrativas de carácter general para el cumplimiento de principios, deberes y derechos reconocidos en la Ley;

XIX. Celebrar convenios con responsables para homologar tratamientos y elevar la protección de datos personales;

XX. Definir y desarrollar el sistema de certificación en materia de protección de datos personales;

XXI. Promover el conocimiento y ejercicio del derecho a la protección de datos personales;

XXII. Diseñar y aplicar indicadores y criterios para evaluar el desempeño de los responsables;

XXIII. Impulsar la capacitación y actualización de responsables;

XXIV. Emitir lineamientos generales para el debido tratamiento de datos personales;

XXV. Emitir lineamientos para homologar el ejercicio de derechos ARCO;

XXVI. Emitir criterios generales de interpretación para garantizar el derecho a la protección de datos personales;

XXVII. Cooperar con autoridades nacionales e internacionales en materia de protección de datos personales;

XXVIII. Promover la tutela del derecho a través de la Plataforma Nacional;

XXIX. Cooperar con otras autoridades nacionales e internacionales para combatir conductas indebidas en el tratamiento de datos personales;

XXX. Diseñar y operar el sistema de buenas prácticas y de certificación en materia de protección de datos personales;

XXXI. Celebrar convenios con Autoridades garantes y responsables para coadyuvar en el cumplimiento de esta Ley; y

XXXII. Ejercer las demás que le confieran esta Ley y otros ordenamientos aplicables.

CAPÍTULO SEGUNDO
DE LAS AUTORIDADES GARANTES

Artículo 82
La integración, designación y funcionamiento de las Autoridades garantes se regirán por lo dispuesto en la Ley de Transparencia y Acceso a la Información Pública del Estado de Baja California Sur y demás disposiciones aplicables.

Artículo 83
Las Autoridades garantes tendrán, además de las atribuciones conferidas por otras leyes, las siguientes:

I. Conocer, sustanciar y resolver los recursos de revisión interpuestos por las personas titulares;

II. Solicitar a la Secretaría que conozca de recursos de interés y trascendencia;

III. Imponer medidas de apremio para asegurar el cumplimiento de sus resoluciones;

IV. Promover y difundir el ejercicio del derecho a la protección de datos personales;

V. Coordinarse con autoridades competentes para garantizar atención en lenguas indígenas;

VI. Garantizar accesibilidad para grupos de atención prioritaria;

VII. Elaborar y publicar estudios e investigaciones en la materia;

VIII. Dar vista a autoridades competentes sobre incumplimientos de la Ley;

IX. Suscribir convenios de colaboración con la Secretaría;

X. Vigilar el cumplimiento de esta Ley en el ámbito de su competencia;

XI. Promover el conocimiento del derecho a la protección de datos personales;

XII. Aplicar indicadores y criterios para evaluar a los responsables;

XIII. Impulsar capacitación y actualización en la materia;

XIV. Solicitar cooperación a la Secretaría conforme a lo previsto en esta Ley; y

XV. Emitir recomendaciones no vinculantes sobre evaluaciones de impacto en la protección de datos personales.

CAPÍTULO TERCERO
DE LA COORDINACIÓN Y PROMOCIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

Artículo 84
Los responsables deberán colaborar con la Secretaría y las Autoridades garantes para capacitar y actualizar permanentemente al personal en materia de protección de datos personales, mediante cursos, talleres y demás formas de enseñanza que se consideren pertinentes.

Artículo 85
La Secretaría y las Autoridades garantes, en el ámbito de sus competencias, deberán:

I. Promover que los planes y programas de estudio incluyan contenidos sobre protección de datos personales y cultura de respeto al derecho;

II. Impulsar, junto con instituciones de educación superior, la creación de centros de investigación, docencia y difusión en la materia; y

III. Fomentar espacios de participación social y ciudadana para el intercambio de ideas entre sociedad, órganos de representación ciudadana y responsables.

TÍTULO NOVENO
DEL PROCEDIMIENTO DE IMPUGNACIÓN

CAPÍTULO PRIMERO
DEL RECURSO DE REVISIÓN

Artículo 86
La persona titular o su representante podrán interponer recurso de revisión ante la Secretaría o las Autoridades garantes, según corresponda, o ante la Unidad de Transparencia que conoció de la solicitud ARCO, dentro de un plazo de quince días hábiles contados a partir del día siguiente a la notificación de la respuesta, por:

I. Escrito libre presentado en el domicilio de la Secretaría o de las Autoridades garantes, o en oficinas habilitadas;

II. Correo certificado con acuse de recibo;

III. Formatos que emitan la Secretaría o las Autoridades garantes;

IV. Medios electrónicos autorizados; o

V. Cualquier otro medio establecido por la autoridad competente.

Se presumirá que la persona recurrente acepta ser notificada por el mismo medio en que interpuso el recurso, salvo que señale uno distinto.

Artículo 87
La identidad de la persona titular podrá acreditarse mediante:

I. Identificación oficial;

II. Firma electrónica avanzada o el instrumento que la sustituya; o

III. Mecanismos de autenticación autorizados por acuerdo publicado en el Boletín Oficial del Gobierno del Estado de Baja California Sur.

El uso de firma electrónica exime de acompañar copia de identificación.

Artículo 88
Si se actúa por representante, éste acreditará su personalidad:

I. Persona física: carta poder simple suscrita ante dos testigos con copias de identificaciones; instrumento público; o comparecencia de titular y representante ante la autoridad;

II. Persona moral: instrumento público.

Artículo 89
Tratándose de datos de personas fallecidas, podrá recurrir quien acredite interés jurídico o legítimo.

Artículo 90
Las notificaciones surten efectos el mismo día en que se practiquen y podrán realizarse:

I. Personalmente, cuando:

a) Sea la primera notificación;

b) Se requiera el cumplimiento de un acto;

c) Se soliciten informes o documentos;

d) Se emita la resolución que ponga fin al procedimiento; o

e) Lo disponga la ley;

II. Por correo certificado con acuse, o por medios digitales o sistemas autorizados mediante acuerdo publicado;

III. Por correo postal ordinario o correo electrónico para actos distintos a los señalados en las fracciones anteriores;

IV. Por estrados, cuando no sea localizable la persona a notificar o se ignore su domicilio.

Artículo 91
Los plazos correrán a partir del día hábil siguiente a aquel en que surta efectos la notificación. Concluidos los plazos, precluirá el derecho para actuar, sin necesidad de acuse de rebeldía.

Artículo 92
La persona titular, el responsable o cualquier autoridad deberán atender los requerimientos de información en los plazos y términos que señalen la Secretaría o las Autoridades garantes.

Artículo 93
Si la persona titular, el responsable o cualquier autoridad no atienden requerimientos, solicitudes, emplazamientos, citaciones o diligencias, o entorpecen actuaciones, perderán su derecho para hacerlo valer posteriormente y la autoridad tendrá por ciertos los hechos materia del procedimiento y resolverá con los elementos disponibles.

Artículo 94
Las partes podrán ofrecer las siguientes pruebas:

I. Documental pública;

II. Documental privada;

III. Inspección;

IV. Pericial;

V. Testimonial;

VI. Confesional, salvo autoridades;

VII. Imágenes, páginas electrónicas, escritos y demás medios tecnológicos;

VIII. Presuncional legal y humana.

La autoridad podrá allegarse de los medios de prueba necesarios, dentro de los límites legales.

Artículo 95
Si no se emite respuesta dentro del plazo del artículo 45, la persona titular o su representante podrán interponer recurso de revisión dentro de los quince días hábiles siguientes al vencimiento del plazo.

Artículo 96
Procede el recurso de revisión cuando:

I. Se clasifiquen como confidenciales datos sin cumplir requisitos legales;

II. Se declare inexistencia de datos personales;

III. Se declare incompetencia del responsable;

IV. Se entreguen datos incompletos;

V. Se entreguen datos distintos a lo solicitado;

VI. Se niegue el acceso, rectificación, cancelación u oposición;

VII. No se responda dentro de plazos legales;

VIII. Se entregue en modalidad o formato distinto al solicitado o incomprensible;

IX. Exista inconformidad con costos de reproducción, envío o tiempos de entrega;

X. Se obstaculice el ejercicio de derechos ARCO pese a su procedencia;

XI. No se dé trámite a la solicitud ARCO; o

XII. Se actualicen otros supuestos previstos en la legislación aplicable.

Artículo 97
El escrito de interposición contendrá, cuando menos:

I. Área responsable ante la cual se presentó la solicitud ARCO;

II. Nombre de la persona recurrente o su representante y, en su caso, del tercero interesado, así como domicilio o medio para notificaciones;

III. Fecha de notificación de la respuesta, o, en su caso, fecha de presentación de la solicitud ARCO;

IV. Acto impugnado, puntos petitorios y motivos de inconformidad;

V. En su caso, copia de la respuesta impugnada y su notificación; y

VI. Documentos que acrediten identidad y, en su caso, representación.

Podrán acompañarse pruebas y elementos que se estimen pertinentes. No se requerirá ratificación del recurso.

Artículo 98
Admitido el recurso, la Secretaría o, en su caso, la Autoridad garante podrá promover conciliación entre la persona titular y el responsable.

Si hay acuerdo, se hará constar por escrito con efectos vinculantes; el recurso quedará sin materia y la autoridad verificará su cumplimiento.

Artículo 99
La conciliación se sujetará a lo siguiente:

I. La autoridad requerirá a las partes que manifiesten su voluntad de conciliar en un plazo de siete días; el acuerdo contendrá un resumen del recurso y, en su caso, de la respuesta del responsable, y señalará puntos de controversia. Podrá celebrarse presencialmente o por medios remotos y se dejará constancia; se exceptúa la conciliación cuando la persona titular sea menor de edad y se hayan vulnerado derechos de la niñez, salvo con representación legal.

II. Con la voluntad de conciliar, se señalará audiencia dentro de los diez días siguientes. La autoridad podrá requerir elementos de convicción en un máximo de cinco días; la audiencia podrá suspenderse una vez, fijando nueva fecha

dentro de cinco días. Se levantará acta de la audiencia; la falta de firma no afectará su validez y se asentará la negativa.

III. Si alguna parte no acude y justifica en tres días, se señalará segunda audiencia dentro de cinco días; si no acude sin justificación, se continuará el procedimiento.

IV. De no haber acuerdo, seguirá el recurso.

V. Si hay acuerdo, se hará constar por escrito con efectos vinculantes y la autoridad verificará su cumplimiento.

VI. El cumplimiento del acuerdo concluye la sustanciación; de lo contrario, la autoridad reanudará el procedimiento.

Artículo 100
La Secretaría o las Autoridades garantes resolverán el recurso en un plazo de cuarenta días hábiles, ampliable por veinte días hábiles por única ocasión.

El plazo se suspenderá durante el cumplimiento del acuerdo de conciliación.

Artículo 101
La autoridad aplicará la suplencia de la queja en favor de la persona titular, sin alterar el contenido original del recurso ni los hechos o peticiones, garantizando el derecho de audiencia de las partes.

Artículo 102
Si el escrito de interposición no cumple los requisitos del artículo 97 y no hay elementos para subsanarlos, la autoridad prevendrá por una sola ocasión para que se subsanen en cinco días hábiles.

La falta de desahogo desechará el recurso. La prevención interrumpe el plazo para resolver, que comenzará a computarse al día hábil siguiente de su desahogo.

Artículo 103
Las resoluciones podrán:

I. Sobreseer o desechar por improcedente;

II. Confirmar la respuesta del responsable;

III. Revocar o modificar la respuesta; o

IV. Ordenar la entrega de datos personales en caso de omisión.

Las resoluciones fijarán plazos y términos para su cumplimiento y los mecanismos de ejecución. Los responsables deberán informar su cumplimiento a la autoridad.

A falta de resolución en plazo, se confirmará la respuesta del responsable.

Si durante la sustanciación se advierte probable responsabilidad por incumplimiento de la Ley, la autoridad dará vista al órgano interno de control o instancia competente.

Artículo 104
El recurso será improcedente y se desechará cuando:

I. Sea extemporáneo;

II. No se acredite identidad o representación;

III. Exista cosa juzgada administrativa;

IV. No se actualice causal del artículo 96;

V. Se tramite un medio de defensa jurisdiccional contra el mismo acto;

VI. La persona recurrente modifique o amplíe su petición sólo respecto de nuevos contenidos; o

VII. No se acredite interés jurídico.

El desechamiento no impide presentar nuevo recurso si sobrevienen elementos distintos.

Artículo 105
Procede el sobreseimiento cuando:

I. La persona recurrente se desista expresamente;

II. La persona recurrente fallezca;

III. Se actualice causal de improcedencia;

IV. El responsable modifique o revoque su respuesta y el asunto quede sin materia; o

V. Quede sin materia por cualquier causa.

Artículo 106
La autoridad deberá notificar a las partes y publicar en versión pública sus resoluciones a más tardar al tercer día hábil siguiente a su emisión.

Artículo 107

Las resoluciones de la Secretaría y de las Autoridades garantes son vinculantes, definitivas e inatacables para los responsables.

Las personas titulares podrán impugnarlas ante los juzgados y tribunales competentes mediante juicio de amparo, en términos de la legislación aplicable.

TÍTULO DÉCIMO
FACULTAD DE VERIFICACIÓN

CAPÍTULO ÚNICO
DEL PROCEDIMIENTO DE VERIFICACIÓN

Artículo 108
La Secretaría y las Autoridades garantes, en el ámbito de sus respectivas competencias, tendrán la atribución de vigilar y verificar el cumplimiento de las disposiciones contenidas en esta Ley y demás normatividad derivada.

En el ejercicio de estas funciones, el personal de la Secretaría o, en su caso, de las Autoridades garantes, estará obligado a guardar confidencialidad sobre la información a la que tenga acceso.

El responsable y/o la persona encargada no podrá negar el acceso a la documentación solicitada con motivo de una verificación ni a sus bases de datos personales, ni invocar reserva o confidencialidad para impedirla.

Artículo 109
La verificación podrá iniciarse:

I. De oficio, cuando existan indicios fundados y motivados de violaciones a la normatividad aplicable; o

II. Por denuncia, cuando la persona titular considere que ha sido afectada por actos del responsable contrarios a esta Ley, o por cualquier persona que tenga conocimiento de presuntos incumplimientos.

El derecho a denunciar precluye al año contado desde el día siguiente a la realización de los hechos u omisiones; si son de tracto sucesivo, el término comenzará a partir del día hábil siguiente al último hecho.

La verificación no procederá en los supuestos de procedencia del recurso de revisión previstos en esta Ley.

Previo a la verificación, la autoridad podrá realizar investigaciones previas para fundar y motivar el acuerdo de inicio.

Artículo 110
Para presentar denuncia no podrán exigirse mayores requisitos que:

I. Nombre de la persona denunciante o, en su caso, de su representante;

II. Domicilio o medio para notificaciones;

III. Relación de hechos y elementos de convicción;

IV. Identificación del responsable denunciado y su domicilio o datos para su ubicación; y

V. Firma de la persona denunciante o, en su caso, de su representante si no sabe firmar, huella digital.

La denuncia podrá presentarse por escrito libre, formatos, medios electrónicos u otros medios que establezcan la Secretaría o las Autoridades garantes. Recibida la denuncia, la autoridad acusará recibo y notificará el acuerdo correspondiente a la persona denunciante.

Artículo 111
La verificación iniciará mediante orden escrita debidamente fundada y motivada, para requerir al responsable y/o persona encargada la documentación e información necesaria vinculada con la presunta violación y/o realizar visitas a oficinas o instalaciones del responsable y/o persona encargada donde estén ubicadas las bases de datos.

Tratándose de instancias de seguridad nacional o seguridad pública, la resolución deberá contener fundamentación y motivación reforzada, asegurándose que la información se utilice exclusivamente por la autoridad y para los fines del artículo 112 de esta Ley.

El procedimiento de verificación tendrá una duración máxima de cincuenta días.

La autoridad podrá dictar medidas cautelares si advierte daño inminente o irreparable en materia de protección de datos, siempre que no impidan el cumplimiento de funciones ni el aseguramiento de bases de datos de los sujetos obligados. Estas medidas serán temporales y con finalidad correctiva, hasta que el sujeto obligado atienda las recomendaciones de la autoridad.

Artículo 112
El procedimiento de verificación concluirá con la resolución que emita la Secretaría o las Autoridades garantes, en la cual se establecerán las medidas que deberá adoptar el responsable, así como el plazo para su cumplimiento.

Artículo 113
Los responsables y/o persona encargada podrán someterse voluntariamente a auditorías practicadas por la Secretaría o las Autoridades garantes, a fin de verificar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados para cumplir esta Ley.

El informe de auditoría dictaminará sobre la adecuación de medidas y controles, identificará deficiencias y propondrá acciones correctivas y/o recomendaciones.

TÍTULO DÉCIMO PRIMERO
MEDIDAS DE APREMIO Y RESPONSABILIDADES

CAPÍTULO PRIMERO
DE LAS MEDIDAS DE APREMIO

Artículo 114
Para el cumplimiento de las resoluciones emitidas por la Secretaría o las Autoridades garantes, se observará lo dispuesto en el Capítulo III del Título Octavo de la Ley De Transparencia y Acceso a la Información Pública del Estado de Baja California Sur.

Artículo 115
La Secretaría o las Autoridades garantes podrán imponer, para asegurar el cumplimiento de sus determinaciones:

I. Amonestación pública, o

II. Multa de 150 hasta 1,500 veces el valor diario de la UMA.

El incumplimiento de los sujetos obligados será difundido en los portales de obligaciones de transparencia de la Secretaría y de las Autoridades garantes, y considerado en las evaluaciones que estas realicen.

Si el incumplimiento implica la presunta comisión de delito o alguna de las conductas sancionables del artículo 125 de esta Ley, la autoridad denunciará ante la instancia competente. Las multas no podrán cubrirse con recursos públicos.

Artículo 116
Si, pese a las medidas de apremio, no se cumple la resolución, se requerirá al superior jerárquico para que, en cinco días siguientes a la notificación, obligue a su cumplimiento sin demora. Transcurrido el plazo sin cumplimiento, se dará vista a la autoridad competente en responsabilidades administrativas.

Artículo 117
Las medidas de apremio serán aplicadas por la Secretaría y las Autoridades garantes, por sí o con apoyo de la autoridad competente.

Artículo 118
Las multas que impongan la Secretaría y las Autoridades garantes se harán efectivas ante la Secretaría de Finanzas y Administración del Gobierno del Estado de Baja California Sur, mediante el procedimiento de cobro coactivo previsto en el Código Fiscal del Estado y Municipios de Baja California Sur.

Artículo 119
Para calificar las medidas de apremio, la autoridad considerará:

I. La gravedad de la falta (daño, indicios de intencionalidad, duración del incumplimiento y afectación a las atribuciones de la autoridad);

II. La condición económica de la persona infractora, y

III. La reincidencia.

La Secretaría o las Autoridades garantes emitirán lineamientos de carácter general sobre atribuciones de las áreas encargadas de calificar la gravedad, notificar y ejecutar las medidas de apremio.

Artículo 120
En caso de reincidencia, la autoridad podrá imponer multa hasta por el doble. Se considerará reincidente quien, habiendo sido sancionado, cometa otra infracción del mismo tipo o naturaleza.

Artículo 121
Las medidas de apremio deberán aplicarse e implementarse en un plazo máximo de quince días, contados desde su notificación a la persona infractora.

Artículo 122
La amonestación pública será impuesta por la autoridad y ejecutada por el superior jerárquico inmediato de la persona infractora.

Artículo 123
La autoridad podrá requerir a la persona infractora la información necesaria para determinar su condición económica; en caso de no proporcionarla, las multas se cuantificarán con base en los elementos disponibles (registros públicos, medios de información, páginas oficiales, etc.). La autoridad podrá requerir información a otras autoridades.

Artículo 124
Contra la imposición de medidas de apremio procede el recurso correspondiente ante los jueces y tribunales del Poder Judicial del Estado.

H. Congreso del Estado de Baja California Sur
Oficialía Mayor
Departamento de Apoyo Parlamentario

Nueva Ley BOGE.88 Extraordinario 24-Diciembre-2025

CAPÍTULO SEGUNDO
DE LAS SANCIONES

Artículo 125. Son causas de sanción por incumplir esta Ley:

I. Actuar con negligencia, dolo o mala fe durante la sustanciación de solicitudes ARCO;

II. Incumplir los plazos para responder solicitudes ARCO o para hacer efectivo el derecho;

III. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar indebidamente datos personales bajo su custodia o a los que tenga acceso por empleo, cargo o comisión;

IV. Dar tratamiento intencional a datos personales en contravención a los principios y deberes de esta Ley;

V. No contar con aviso de privacidad o omitir elementos del artículo 21 de esta Ley;

VI. Clasificar como confidenciales, con dolo o negligencia, datos personales sin cumplir los requisitos legales la sanción procede cuando exista resolución firme sobre el criterio de clasificación;

VII. Incumplir el deber de confidencialidad del artículo 36;

VIII. No establecer medidas de seguridad conforme a los artículos 25, 26 y 27;

IX. Presentar vulneraciones por falta de implementación de medidas de seguridad;

X. Efectuar transferencias de datos personales en contravención a esta Ley;

XI. Obstruir actos de verificación;

XII. Crear bases de datos en contravención al artículo 5;

XIII. No acatar resoluciones de la Secretaría o de las Autoridades garantes, y

XIV. Omitir el informe anual y demás informes a que se refiere el artículo 40, fracción VI, de la Ley General de Transparencia y Acceso a la Información Pública, o presentarlos extemporáneamente.

Las conductas de las fracciones I, II, IV, VI, X, XII y XIV, así como la reincidencia en las demás, se considerarán graves para efectos de sanción administrativa.

Si la presunta infracción la comete un integrante de partido político, la investigación y sanción corresponderán a la autoridad electoral competente.

Las sanciones económicas no podrán cubrirse con recursos públicos.

Artículo 126
Para las conductas del artículo anterior, se dará vista a la autoridad competente para que imponga o ejecute la sanción.

Artículo 127
Las responsabilidades administrativas a que se refiere el artículo 125 son independientes de las civiles, penales u otras que puedan derivar de los mismos hechos. Se determinarán y ejecutarán conforme a los procedimientos y autoridades previstos en las leyes aplicables.

La Secretaría o las Autoridades garantes podrán denunciar ante autoridades competentes cualquier acto u omisión violatoria de esta Ley, aportando las pruebas pertinentes.

Artículo 128
Ante incumplimientos de partidos políticos, la Secretaría o la Autoridad garante dará vista al Instituto Estatal Electoral de Baja California Sur, para lo conducente, sin perjuicio de las sanciones aplicables a dichos institutos.

En probables infracciones de fideicomisos o fondos públicos, la autoridad dará vista al órgano interno de control o equivalente del sujeto obligado.

Artículo 129
Si la persona presunta infractora es servidora pública, la Secretaría o la Autoridad garante remitirá a la autoridad competente la denuncia y un expediente con todos los elementos que sustenten la presunta responsabilidad administrativa.

La autoridad que conozca informará la conclusión del procedimiento y, en su caso, la ejecución de la sanción.

Para ello, la Secretaría o la Autoridad garante elaborará:

I. Denuncia dirigida a la contraloría, órgano interno de control o equivalente, con la descripción precisa de actos u omisiones; y

II. Expediente con las pruebas pertinentes que acrediten el nexo causal entre hechos y pruebas.

La denuncia y el expediente deberán remitirse dentro de los quince días siguientes a que la autoridad tenga conocimiento de los hechos.

Artículo 130
La Autoridad garante deberá denunciar ante la autoridad competente el incumplimiento de sus determinaciones que presuman la comisión de un delito.

T R A N S I T O R I O S

PRIMERO. El presente Decreto entrará en vigor el día 01 de enero de 2026, previa su publicación en el Boletín Oficial del Gobierno del Estado de Baja California Sur.

SEGUNDO. Se abroga la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Baja California Sur expedida por el Congreso del Estado mediante decreto número 2461 y publicada en el Boletín Oficial del Gobierno del Estado de Baja California Sur de fecha 17 de julio de 2017.

Asimismo, se derogan todas las disposiciones de igual o menor jerarquía que se opongan o contravengan lo dispuesto en el presente Decreto.

TERCERO. El Titular del Poder Ejecutivo, por conducto de la Secretaría de la Contraloría y Transparencia Gubernamental deberá expedir el Reglamento de esta Ley y los lineamientos generales necesarios para su implementación a más tardar el 31 de diciembre de 2025.

CUARTO. En términos del Decreto Número 3178 de reforma constitucional local, a partir de la entrada en vigor de este decreto se entenderá extinto el Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Baja California Sur. La Secretaría asumirá las funciones previstas en esta Ley y las Autoridades garantes ejercerán las atribuciones que les confiere el Título Octavo.

QUINTO. El comité de Transición a que hace alusión el régimen transitorio de la nueva Ley de Transparencia y Acceso a La Información Pública del Estado de Baja California Sur, tendrá también la responsabilidad de llevar a cabo todas las acciones que resulten necesarias para dar paso a las obligaciones que en materia de protección de datos personales en posesión de sujetos obligados tendrá la Secretaría de la Contraloría y Transparencia Gubernamental.

SEXTO. Los procedimientos, recursos de revisión, verificaciones, denuncias, medidas de apremio, sanciones y demás asuntos en trámite a la entrada en vigor de esta Ley continuarán sin interrupción ante la Secretaría o la Autoridad competente, conservando su estado procesal y plazos. Los actos válidamente realizados conservarán su eficacia jurídica.

SÉPTIMO. Los sujetos obligados deberán:

a) Ajustar su aviso de privacidad integral y simplificado a los artículos 20 a 22, dentro de 90 días naturales;

b) Contar con Documento de Seguridad, inventario de tratamientos y bitácora de vulneraciones conforme a los artículos 27 a 33, dentro de 120 días naturales.

OCTAVO. Los contratos, convenios o instrumentos con personas encargadas o proveedores de cómputo en la nube deberán adecuarse a los artículos 53, 57 y 58 de esta Ley dentro de los 180 días naturales siguientes a su publicación, incorporando cláusulas de confidencialidad, seguridad, supresión y transparencia en subcontrataciones.

NOVENO. Los sujetos obligados que ya operen tratamientos intensivos o relevantes deberán elaborar y presentar la Evaluación de Impacto en Protección de Datos Personales prevista en el artículo 68 dentro de los 180 días naturales siguientes a la publicación de esta Ley, salvo los supuestos de excepción del artículo 73, debidamente fundados y motivados.

DÉCIMO. La Secretaría emitirá, a más tardar el 31 de diciembre de 2025, lineamientos sobre:

I. Avisos de privacidad;

II. Ejercicio de derechos ARCO y portabilidad;

III. Medidas de seguridad administrativa, física y técnica;

IV. Procedimiento de verificación;

V. Mejores prácticas y certificación;

VI. Evaluación de impacto; y

VII. Transferencias y remisiones.

DÉCIMO PRIMERO. Los sujetos obligados deberán asegurar la operación continua e interoperabilidad con la Plataforma Nacional de Transparencia, garantizando la migración y actualización de cuentas, perfiles y módulos vinculados al ejercicio de derechos ARCO en un plazo de 60 días naturales contados desde la publicación de esta Ley.

DÉCIMO SEGUNDO. La Secretaría de Finanzas y Administración del Gobierno del Estado de Baja California Sur, deberá proveer para el año 2026 los recursos suficientes y necesarios para el cumplimiento de este Decreto.

DÉCIMO TERCERO. Todas las referencias normativas a la "Autoridad garante estatal" o al "Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Baja California Sur" contenidas en leyes, reglamentos, decretos, acuerdos o cualquier disposición, se entenderán hechas a la Secretaría y a las Autoridades garantes a que se refiere esta Ley, según sus competencias.

DÉCIMO CUARTO. En lo que no se oponga a la presente Ley, permanecerán vigentes los criterios, acuerdos y lineamientos técnicos del Instituto extinto y de autoridades federales competentes, hasta en tanto la Secretaría emita las disposiciones locales correspondientes.

DADO EN EL SALÓN DE SESIONES DEL PODER LEGISLATIVO, EN LA PAZ, BAJA CALIFORNIA SUR, A LOS 11 DÍAS DEL MES DE DICIEMBRE DEL AÑO 2025. Presidenta.- Dip. María Cristina Contreras Rebollo.- Rúbrica. **Secretaria.-** Dip. Karina Olivas Parra.- Rúbrica.