

REGLAMENTO DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS PARA EL MUNICIPIO DE BENITO JUÁREZ, QUINTANA ROO

Publicado en el POE Núm. 20 Ext. del 02 de febrero de 2022

ACUERDO 21-24/012

SEXTO PUNTO DEL ORDEN DEL DÍA DE LA SEXTA SESIÓN ORDINARIA, DE FECHA 02 DE DICIEMBRE DEL 2021, EN EL QUE SE APRUEBA POR UNANIMIDAD DE VOTOS DE LOS INTEGRANTES DEL HONORABLE AYUNTAMIENTO CONSTITUCIONAL DEL MUNICIPIO DE BENITO JUÁREZ, QUINTANA ROO, 2021-2024, EL DICTAMEN DE LA INICIATIVA POR LA QUE SE EXPIDE EL REGLAMENTO DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS PARA EL MUNICIPIO DE BENITO JUÁREZ, QUINTANA ROO, EN LOS TÉRMINOS DEL PROPIO ACUERDO.-----

El Honorable Ayuntamiento Constitucional del Municipio de Benito Juárez, Quintana Roo, 2021-2024, con fundamento en los artículos 115 y demás relativos de la Constitución Política de los Estados Unidos Mexicanos; 126, 133, 145 y demás relativos de la Constitución Política del Estado Libre y Soberano de Quintana Roo; 1º, 2º, 3º, 7º, 65, 66 fracción I incisos b) y c) y 68, 69, 70, 72 fracción I, 74, 87, 93 fracciones V y VII, 221, 223, 224, 225 y demás relativos y aplicables de la Ley de los Municipios del Estado de Quintana Roo; 1º, 2º, 3º, 5º, 6º fracción I, 8º, 73, 74, 92, 93 fracciones VII y X, 102, 103, 104, 105, 135, y demás aplicables del Bando de Gobierno y Policía del Municipio de Benito Juárez, Quintana Roo; 1º, 2º, 5º, 6º, 26, 31, 32, fracciones III y IV, 33, 86, 98 fracción I, II y VIII, 105, 106 fracciones VII y X, 114 fracción I, 117, fracción I, 139, 156 y demás relativos y aplicables del Reglamento del Gobierno Interior del Ayuntamiento del Municipio de Benito Juárez, Quintana Roo; y,

CONSIDERANDO

Que las Comisiones Unidas de Gobierno, Régimen Interior y Anticorrupción y de Mejora Regulatoria, Transparencia, Protección de Datos Personales y Acceso a la Información Pública, en seguimiento al trámite acordado en el desahogo del octavo punto del orden del día de la Segunda Sesión Ordinaria de este Honorable Ayuntamiento Constitucional del Municipio de Benito Juárez, Quintana Roo, 2021-2024, de fecha siete de octubre de dos mil veintiuno, se abocaron al estudio y análisis de la Iniciativa por la que se expide el Reglamento de Protección de Datos Personales en Posesión de Sujetos Obligados para el Municipio de Benito Juárez, Quintana Roo, presentada por el Ciudadano Jorge Arturo Sanen Cervantes, Regidor Presidente de la Comisión de Desarrollo Social, Participación Ciudadana y Derechos Humanos.

Que el referido dictamen fue remitido a la Secretaria General del Ayuntamiento para los efectos conducentes, mismo que en esta oportunidad se somete a la consideración del H. Ayuntamiento, y que es del siguiente tenor literal:

HONORABLE AYUNTAMIENTO CONSTITUCIONAL DEL MUNICIPIO DE BENITO JUÁREZ, QUINTANA ROO, 2021-2024 P R E S E N T E

Los ciudadanos Regidores integrantes de las Comisiones Unidas de Gobierno, Régimen Interior y Anticorrupción y de Mejora Regulatoria, Transparencia, Protección de Datos Personales y Acceso a la Información Pública, con fundamento y en ejercicio de las

facultades que nos confieren los artículos 115 de la Constitución Política de los Estados Unidos Mexicanos; 126, 133, 145 y demás relativos y aplicables de la Constitución Política del Estado Libre y Soberano de Quintana Roo; 1º, 2º, 3º, 7º, 65, 66 fracción I incisos b) y c), 68, 69, 70, 72 fracción I, 74, 87, 93 fracciones III y IV, 221, 223, 224, 225 y demás aplicables de la Ley de los Municipios del Estado de Quintana Roo; 1º, 2º, 3º, 5º, 6º fracción I, 8º, 73, 74, 92, 93 fracciones VII y X, 102, 103, 104, 105, 135, 241, y demás aplicables del Bando de Gobierno y Policía del Municipio de Benito Juárez, Quintana Roo; 1º, 2º, 5º, 6º, 26, 31, 32 fracciones III y IV, 33, 86, 98 fracciones I y II, 105, 106 fracciones VII y X, 114 fracción I, 117, fracción I, 139, 156, 157, 158, 159, y demás relativos y aplicables del Reglamento del Gobierno Interior del Ayuntamiento del Municipio de Benito Juárez, Quintana Roo, venimos a someter a la consideración de este Órgano Colegiado de Gobierno Municipal, el dictamen de la Iniciativa por la que se expide el Reglamento de Protección de Datos Personales en Posesión de Sujetos Obligados para el Municipio de Benito Juárez, Quintana Roo, el cual deriva de los siguientes:

ANTECEDENTES

En el desahogo del octavo punto del orden del día de la Segunda Sesión Ordinaria de este Honorable Ayuntamiento Constitucional del Municipio de Benito Juárez, Quintana Roo, 2021-2024, de fecha siete de octubre de dos mil veintiuno, se dio trámite a la Iniciativa por la que se expide el Reglamento de Protección de Datos Personales en Posesión de Sujetos Obligados para el Municipio de Benito Juárez, Quintana Roo, presentada por el Ciudadano Jorge Arturo Sanen Cervantes, Regidor Presidente de la Comisión de Desarrollo Social, Participación Ciudadana y Derechos Humanos.

Con fundamento en el artículo 153 del Reglamento del Gobierno Interior del Ayuntamiento del Municipio de Benito Juárez, Quintana Roo, la referida iniciativa fue remitida para su estudio, valoración y dictamen a las Comisiones Unidas de Gobierno, Régimen Interior y Anticorrupción y de Mejora Regulatoria, Transparencia, Protección de Datos Personales y Acceso a la Información Pública.

Mediante oficio número SG/DGUTJyD/015/2021, de fecha siete de octubre de dos mil veintiuno, la Secretaría General del Ayuntamiento, remitió a las suscritas Comisiones Unidas, la Iniciativa objeto del presente dictamen.

Que, en cumplimiento a lo anterior, los integrantes de las Comisiones Unidas de Gobierno, Régimen Interior y Anticorrupción y de Mejora Regulatoria, Transparencia, Protección de Datos Personales y Acceso a la Información Pública, tenemos a bien emitir el dictamen de la Iniciativa por la que se expide el Reglamento de Protección de Datos Personales en Posesión de Sujetos Obligados para el Municipio de Benito Juárez, Quintana Roo, mismo que se formuló en atención a las siguientes:

CONSIDERACIONES

Que la autonomía del Municipio libre se expresa en la facultad de gobernar y administrar por sí mismo los asuntos propios de su comunidad, en el ámbito de competencia que le señala la Constitución Política de los Estados Unidos Mexicanos y las leyes que conforme a ella se expidan;

Que en ese tenor, los Ayuntamientos tienen facultades para formular, aprobar y publicar, de acuerdo con las Leyes en materia municipal que expida la Legislatura del Estado, el Bando de Gobierno y Policía, los Reglamentos, circulares y disposiciones administrativas de observancia general dentro de sus respectivas jurisdicciones, que organicen la administración pública municipal, regulen las materias, procedimientos, funciones y servicios públicos de su competencia y aseguren la participación ciudadana y vecinal;

Que las Comisiones Unidas de Gobierno, Régimen Interior y Anticorrupción y de Mejora Regulatoria, Transparencia, Protección de Datos Personales y Acceso a la Información Pública, son competentes para dictaminar la Iniciativa objeto del presente documento, en atención a lo previsto en los artículos 92 del Bando de Gobierno y Policía del Municipio de Benito Juárez, Quintana Roo, y 86, 105, 114 fracción I y 117 fracción I, del Reglamento del Gobierno Interior del Ayuntamiento del Municipio de Benito Juárez, Quintana Roo;

Qué, asimismo, el presente Dictamen se formuló de conformidad al procedimiento y formas establecidas en los artículos 129 a 136, 157, 158 y 159 del Reglamento del Gobierno Interior del Ayuntamiento del Municipio de Benito Juárez, Quintana Roo;

Que la iniciativa que se dictamina en lo medular señala:

...

El derecho a la protección de datos personales es un derecho fundamental autónomo y distinto al resto de los derechos fundamentales que, si bien puede guardar una cercana relación con derechos como el de privacidad e intimidad, posee características propias y por tanto tiene objetivos e implicaciones diversas; está asociado a la evolución tecnológica que vivimos en nuestros días, en la que el flujo de información personal es incuantificable; fue necesaria la generación de un nuevo derecho o a la autodeterminación informativa que respondiera de manera efectiva a los retos que el uso de los datos personales al surgir los desarrollos tecnológicos con la finalidad de dotar a las personas de un instrumento idóneo que les permitiera hacer frente a los efectos producidos por los desarrollos informáticos en el tratamiento de los datos personales.

Desde el 2002, con la expedición de la Ley Federal de Transparencia, se incorporó el derecho a la protección de datos personales en el marco jurídico mexicano, como limitante al derecho de acceso a la información; es en el año 2005 que se publicaron en el DOF los Lineamientos de Protección de Datos Personales, los cuales representan una regulación sin precedentes en México al ser primer instrumento normativo, que desarrolla aspectos sustantivos en la materia tales como principios, deberes y derechos.

A partir de 2006, en el contexto de la reforma al artículo 6° CPEUM, en materia de transparencia y acceso a la información, se hace la primera referencia constitucional al derecho a la protección de datos personales, pero sin regularlo sustancialmente, reiterando el papel de este derecho como contrapeso del derecho de acceso a la información.

Para el 7 de febrero de 2014 se publicó en el DOF el Decreto por el que se reforman y adicionan diversas disposiciones de la CPEUM, en materia de transparencia; esta iniciativa tiene el objeto de conformar la legislación secundaria que desarrolla el

contenido del derecho a la protección de datos personales que reconoce nuestra Carta Magna.

Es así que por la estrecha relación que existe entre el derecho a la privacidad y a la intimidad con el derecho de protección de datos personales, este derecho se dotó de contenido, una adición de un párrafo segundo al artículo 16 constitucional dejando como manifiesto que el derecho de protección de datos personales es un derecho distinto y autónomo de otros derechos humanos.

Por lo narrado que la reforma constitucional establece en su artículo segundo transitorio el mandato al Congreso de la Unión para “expedir la Ley General del Artículo 6° de la CPEUM en relación con el artículo 73, fracción XXIX-S que establece la obligación para “expedir las leyes generales reglamentarias que desarrollen los principios y bases en materia de transparencia gubernamental, acceso a la información y protección de datos personales en posesión de las autoridades, entidades, órganos y organismos gubernamentales de todos los niveles de gobierno.

La presentación de esta iniciativa responde al mandato constitucional y la apremiante urgencia de una reglamentación que permita el desarrollo del derecho de protección de datos personales; al contar con una norma secundaria aplicable a nivel nacional; teniendo consigo entre las novedades la aplicación de sujetos obligados , refiere como universo a cualquier autoridad, entidad, órgano u organismo, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal.

Que el presente reglamento tiene como objetivo el diseño, la ejecución y evaluación de un programa municipal de protección de datos personales que defina la política pública, y en función de la misma, se desarrollen instrumentos y acciones concretas para:

- 1. Consolidar una cultura de protección de datos personales*
- 2. Fomentar el ejercicio del derecho a la protección de datos personales.*
- 3. Capacitar a los servidores públicos.*
- 4. Establecer mecanismos que midan, reporten y verifiquen las metas establecidas en el sistema nacional de transparencia*

Se establece que las medidas de seguridad para el tratamiento de datos personales deben estar documentadas y contenidas en un sistema de gestión, que permita operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales de conformidad con lo previsto en la ley genera y las demás disposiciones que le resulten aplicables.

A su vez se prevé la regulación de los derechos de acceso, rectificación, cancelación y oposición, comúnmente reconocidos por su acrónimo como derechos ARCO cabe destacar que debido a que como regla general los entes y organismos del sector público llevan a cabo el tratamiento de datos personales habilitados por una norma o disposición jurídica, el derecho de los titulares a suprimir su información y a oponerse a su tratamiento, se circunscribe a aquellos casos que actualicen las hipótesis previstas en el presente reglamento.

De igual forma se establecen las reglas básicas para la realización de transferencias y remisiones de datos personales; se contaría con reglas que de manera clara establecen el mecanismo a través de cual se puede transferir información válidamente, dentro y fuera del Municipio de Benito Juárez, a través de sus sujetos obligados, por otra parte, se propone la adopción de esquemas mínimos de mejores prácticas con la finalidad de:

- 1. Elevar el nivel de protección de los datos personales.*
- 2. Armonizar el tratamiento de datos personales*
- 3. Facilitar el ejercicio de los derechos ARCO.*
- 4. Complementar las disposiciones previstas en la normatividad que resulte aplicable*
- 5. Demostrar ante el Instituto o, en su caso, los organismos garantes, el cumplimiento en materia de datos personales.*

...

Que las Comisiones Unidas de Gobierno, Régimen Interior y Anticorrupción y de Mejora Regulatoria, Transparencia, Protección de Datos Personales y Acceso a la Información Pública, concluyen que la iniciativa que se dictamina es de aprobarse en lo general, toda vez que deviene imperante contar con un ordenamiento jurídico que contenga el diseño, la ejecución y evaluación de un programa municipal de protección de datos personales que defina la política pública, y en función de la misma, se desarrollen instrumentos y acciones concretas para consolidar una cultura de protección de datos personales, fomentar el ejercicio del derecho a la protección de datos personales, capacitar a los servidores públicos, así como establecer mecanismos que midan, reporten y verifiquen las metas establecidas en el sistema nacional de transparencia.

Que sin embargo, en lo particular, las Comisiones Dictaminadoras, consideraron pertinente realizar diversas adecuaciones y precisiones en la redacción y contenido de algunos de los artículos de la iniciativa, a fin de brindar mayor claridad en la interpretación y para la aplicación de estos.

Que, por todo lo antes expuesto y fundado, las Comisiones Unidas de Gobierno, Régimen Interior y Anticorrupción y de Mejora Regulatoria, Transparencia, Protección de Datos Personales y Acceso a la Información Pública, tiene a bien emitir los siguientes puntos:

RESOLUTIVOS

PRIMERO. - Se aprueba expedir el Reglamento de Protección de Datos Personales en Posesión de Sujetos Obligados para el Municipio de Benito Juárez, Quintana Roo, para quedar de conformidad a lo siguiente:

REGLAMENTO DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS PARA EL MUNICIPIO DE BENITO JUÁREZ, QUINTANA ROO.

Publicado en el POE Núm. 20 Ext. del 02 de febrero de 2022

TÍTULO PRIMERO Disposiciones Generales

Capítulo Único Del Objeto

Artículo 1. El presente reglamento es de orden público, de observancia general en todo el Municipio de Benito Juárez, del Estado de Quintana Roo, tiene por objeto; establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de los sujetos obligados.

Artículo 2. Son sujetos obligados, cualquier autoridad, entidad, órgano y organismo público autónomos, fideicomisos, fondos públicos, en consideración a las bases y procedimientos establecidos en la Ley general, en la ley y el presente reglamento.

Las personas físicas, morales y/o sindicatos que reciban y ejerzan recursos públicos o realicen actos de autoridad de la administración pública municipal, serán responsables de los datos personales, de conformidad con la normativa aplicable para la protección de datos personales en posesión de los particulares.

Artículo 3. Son objetivos del presente Reglamento:

- I.- Garantizar que toda persona pueda ejercer el derecho a la protección de los datos personales;
- II.- Proteger los datos personales en posesión de cualquier autoridad, entidad, órgano, organismo público autónomo, fideicomisos y fondos públicos del municipio, con la finalidad de regular su debido tratamiento;
- III.- Establecer las bases mínimas y condiciones homogéneas que rijan 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 el presente reglamento y demás disposiciones que resulten aplicables en la materia;
- V.- Promover, fomentar y difundir una cultura de protección de datos personales;
- VI.- Vigilar la implementación, mantenimiento y actualización de medidas de seguridad con carácter administrativo, técnico y físico que permitan la protección de los datos personales,
- VII.- Establecer los mecanismos para garantizar el cumplimiento y la efectiva aplicación de las medidas de apremio que correspondan para aquellas conductas que contravengan las disposiciones previstas en materia de protección de datos personales.

Artículo 4. Para los efectos de la presente ley se entenderá por:

- I.- **Áreas:** Instancias responsables previstas en los respectivos reglamentos, estatutos orgánicos o instrumentos equivalentes, que cuentan o pueden contar, dar tratamiento, y ser responsable o encargadas de los datos personales;
- II.- **Aviso de Privacidad:** Documento o disposición del titular de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle

los propósitos del tratamiento de los mismos;

- III.- **Bases de datos:** Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados que permitan su tratamiento, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento u organización;
- IV.- **Bloqueo:** La 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 estas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido este, se procederá a su supresión en las bases de datos, archivo, registro, expediente o sistema de información que corresponda;
- V.- **Comité de Transparencia:** Instancia a la que hace referencia el artículo 95 de la Ley, artículo 36 del reglamento de transparencia y artículo 100 del presente reglamento.
- VI.- **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;
- VII.- **Consejo Nacional:** Consejo Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales a que se refiere el Artículo 32 de la Ley General de Transparencia;
- VIII.- **Consentimiento:** Manifestación de la voluntad libre, específica e informada del titular mediante la cual autoriza el tratamiento de sus datos personales;
- IX.- **Datos personales:** Cualquier información concerniente a una persona física identificada o identificable expresada en forma numérica, alfabética, alfanumérica, gráfica, fotográfica, acústica o en cualquier otro formato. 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 éste. Se consideran sensibles de manera enunciativa más no limitativa, los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud pasado, presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas, datos biométricos, preferencia sexual y de género;
- XI.- **Derechos ARCO:** Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de los datos personales;
- XII.- **Días:** Días hábiles;
- XIII.- **Disociación:** El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su lectura, contenido o grado de desagregación, la identificación del mismo;
- XIV.- **Documento de seguridad:** Instrumento que describe y da cuenta de manera

general sobre las medidas de seguridad de carácter técnico, físico y administrativo adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee;

- XV.- Encargado:** La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o adjuntamente con otras, trata datos personales a nombre y por cuenta del responsable;
- XVI.- Enlace:** Servidor público responsable ante la Unidad de Transparencia de tramitar, procesar, atender las solicitudes de derecho Arco, Avisos de privacidad, Medidas de seguridad físicas, técnicas y administrativa en materia de protección de datos personales;
- XVII.- Evaluación de impacto en la protección de datos personales:** Documento mediante el cual los Responsables 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, se valoran y determinan los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar, prevenir y mitigar posibles riesgos que puedan comprometer el cumplimiento de los principios, deberes, derechos de los titulares, así como los deberes de los responsables y encargados previstos en la norma aplicable;
- XVIII.- Fuentes de acceso público:** Aquellas bases de datos, sistemas o archivos que 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 considera fuente de acceso público cuando los datos personales contenidos en la misma sean obtenidos o tengan una procedencia ilícita, conforme a las disposiciones establecidas por la normativa aplicable;
- XIX.- Instituto:** Instituto de Acceso a la Información y Protección de Datos Personales de Quintana Roo;
- XX.- Instituto Nacional:** Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales;
- XXI.- Ley:** Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Quintana Roo;
- XXII.- Ley General:** Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;
- XXIII.- Ley General de Transparencia:** Ley General de Transparencia y Acceso a la Información Pública;
- XXIV.- Ley de Transparencia:** Ley de Transparencia y Acceso a la Información Pública para el Estado de Quintana Roo;
- XXV.- Lineamientos Generales.** Lineamientos Generales de Protección de Datos Personales para el Sector Público;
- XXVI.- Medidas Compensatorias:** Mecanismos alternos para dar a conocer a los titulares el aviso de privacidad, a través de su difusión por medios masivos de comunicación u otro de amplio alcance;

- XXVII.- Medidas de seguridad:** Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales;
- XXVIII.- Medidas de seguridad administrativas:** Políticas y procedimientos para la gestión, soporte y revisión de la seguridad a nivel organizacional, identificación, clasificación y borrado seguro, así como la sensibilización y capacitación del personal en materia de protección de datos personales;
- XXIX.- 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. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:
- a).- Prevenir el acceso no autorizado al perímetro de la organización del responsable, sus instalaciones físicas, áreas críticas, recurso 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 del responsable; y,
 - d).- Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.
- XXX.- 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 los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:
- a).- Prevenir que el acceso a las bases de datos personales, así como a los recursos, sea por usuarios identificados y autorizados;
 - b).- Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo 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.
- XXXI.- Plataforma Nacional:** La Plataforma Nacional de Transparencia a que hace referencia el artículo 49 de la Ley General de Transparencia;
- XXXII.- Reglamento de Transparencia:** Reglamento de Transparencia y Acceso a la Información Pública para el Municipio de Benito Juárez, Quintana Roo;
- XXXIII.- Remisión:** Toda la comunicación de datos personales realizada exclusivamente entre el responsable y encargado, con independencia que se realice dentro o fuera del Municipio de Benito Juárez, Quintana Roo;
- XXXIV.- Responsable:** Los sujetos obligados a que se refiere el artículo 2 de la Ley y del presente reglamento que decidan sobre el tratamiento de datos personales; es

decir la persona física, jurídica, autoridad pública, servicio u organismo que solo o conjuntamente determinen los fines, alcance y medios del tratamiento de datos personales;

- XXXV.- Sistema Nacional:** El Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales;
- XXXVI.- Sujetos Obligados:** Son los actores a los que les aplica la Ley General, la Ley, el presente reglamento, responsables del cumplimiento de las disposiciones en materia de protección de datos personales; es decir cualquier persona física o moral que reciba, ejerza recursos públicos y/o que ejerza actos de autoridad;
- XXXVII.- Supresión:** La baja archivista de los datos personales conforme a la normativa archivista aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable;
- XXXVIII.- Titular:** La persona física a quien correspondan los datos personales;
- XXXIX.- Transferencia:** Toda comunicación de datos personales dentro o fuera del territorio del Municipio de Benito Juárez, Quintana Roo, realizada a persona distinta del titular, del responsable o del encargado;
- XL.- Tratamiento:** Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionados de manera enunciativa más no limitativa con la obtención, uso, registro, organización, conservación, elaboración, utilización, estructuración, adaptación, modificación, extracción, consulta, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia y en general cualquier uso o disposición de datos personales;
- XLI.- Unidades Administrativas:** Estructura básica de un sujeto obligado en caso de contar con ella, facultada para llevar a cabo actividades que conduzcan al cumplimiento de objetivos del presente reglamento y metas establecidas en los programas en materia de protección de datos personales; y,
- XLII.- Unidad de Transparencia:** Unidad de Transparencia, Acceso a la información y Protección de Datos Personales, del Municipio de Benito Juárez, Quintana Roo.

Artículo 5. La aplicación e interpretación del presente reglamento se realizará conforme a lo dispuesto por 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 Quintana Roo, así como las resoluciones y sentencias vinculantes que emiten los órganos nacionales e internacionales y la Ley General, favoreciendo en todo tiempo el derecho a la privacidad, la protección de datos personales y a las personas la protección más amplia.

Para el caso de la interpretación, se podrán tomar en cuenta los criterios, determinaciones y opiniones de los organismos nacionales e internacionales especializados, privilegiando en todo momento la interpretación que más favorezca al titular.

Artículo 6. El presente reglamento será aplicable a cualquier tratamiento de datos

personales que obren en soportes físicos o electrónicos, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Artículo 7. Para los efectos de este reglamento, se entenderán como fuentes de acceso público:

- I.- Las páginas de internet o medios remotos o locales de comunicación electrónica, óptica y de otra tecnología, siempre que el sitio donde se encuentren los datos personales esté concebido para facilitar información al público y esté abierto a la consulta general;
- II.- Los directorios telefónicos en términos de la normatividad específica;
- III.- Los diarios, gacetas o boletines oficiales, de acuerdo con su normativa;
- IV.- Los medios de comunicación social; y,
- V.- Los registros públicos conforme a las disposiciones que resulten aplicables.

Para que los supuestos enumerados en el presente 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 una fuente de acceso público cuando la información contenida en la misma sea o tenga una procedencia ilícita.

Artículo 8. Los Sujetos Obligados a través de sus unidades administrativas 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 se limitará por razones de orden público, seguridad pública, salud pública o para proteger los derechos de terceros.

Artículo 9. Por regla general no podrán tratarse datos personales sensibles, salvo que se cuente con el consentimiento expreso de su titular o en su defecto, se trate de los casos establecidos en el Artículo 19 de este Reglamento.

En el tratamiento de datos personales de menores de edad se deberá privilegiar el interés superior de las niñas, niños y los adolescentes, en términos de las disposiciones legales aplicables.

Artículo 10. A falta de disposición expresa en el presente reglamento, se aplicarán de manera supletoria las disposiciones siguientes:

- I. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
- II. Ley General de Transparencia y Acceso a la Información Pública;
- III. Ley de Transparencia y Acceso a la Información Pública para el Estado de Quintana Roo
- IV. Código Civil para el Estado Libre y Soberano de Quintana Roo;
- V. Código de Procedimientos Civiles para el Estado Libre y Soberano de Quintana Roo; y,
- VI. Las leyes, reglamentos y lineamientos de orden común que resulten aplicables.

TÍTULO SEGUNDO Principios y Deberes

Capítulo I De los Principios

Artículo 11. El responsable deberá observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los datos personales.

Artículo 12. El tratamiento de datos personales por parte del responsable deberá sujetarse a las facultades y atribuciones que la normativa aplicable les confiere, se concibe así el principio de licitud.

No deben tratarse datos personales si no se tienen facultades previamente otorgadas, en este sentido el responsable solo podrá hacer con los datos personales aquello que este legalmente permitido como acto de autoridad.

Artículo 13. Todo tratamiento de datos personales que efectuó el responsable deberá estar justificado contando con fines concretos, lícitas, explícitas y legítimas, en relación con las atribuciones expresas que la normatividad aplicable les confiera, entendiéndose como el principio de Finalidad.

Es el propósito, motivo o razón por el cual se tratan los datos personales, que ha sido informado al titular en el aviso de privacidad y en su caso consentidas por este y deben ser:

- a).- **Concretas:** Cuando el tratamiento de los datos personales atiende a la consecución de fines específicos o determinados, sin que sea posible la existencia de finalidades genéricas que puedan ocasionar confusión en el titular;
- b).- **Explícitas:** Cuando las finalidades se expresan y dan a conocer de manera clara en el aviso de privacidad;
- c).- **Lícitas** cuando las finalidades que justifican el tratamiento de los datos personales son acordes con las atribuciones expresas del responsable, conforme a lo previsto en la legislación mexicana y el derecho internacional que le resulte aplicable; y,
- d).- **Legítimas:** Se encuentren habilitadas por el consentimiento del titular, salvo que se actualice alguna de las causales previstas en el artículo 19 del presente reglamento.

El responsable podrá tratar datos personales para finalidades distintas a aquellas establecidas en el aviso de privacidad, siempre y cuando cuente con atribuciones conferidas por ley y medie el consentimiento del titular, salvo que sea una persona reportada como desaparecida, en los términos previstos de las disposiciones que resulten aplicables a la materia.

Artículo 14. El responsable no deberá obtener y tratar datos personales, a través de medios engañosos o fraudulentos, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad; generando así el principio de lealtad.

Se entenderá que el responsable actúa de forma engañosa o fraudulenta cuando:

- I.- Medie dolo, mala fe o negligencia en el tratamiento de datos personales que lleve a cabo;

- II.- Realice un tratamiento de datos personales que dé lugar a una discriminación injusta o arbitraria contra el titular, o
- III.- Vulnere la expectativa razonable de protección de datos personales.

Artículo 15. Cuando no se actualice algunas de las causales de excepción previstas en el artículo 19 del presente reglamento, el responsable deberá contar con el consentimiento previo del titular para el tratamiento de los datos personales, el cual deberá otorgarse de forma:

- I.- **Libre:** Sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular;
- II.- **Específica:** Referida a finalidades concretas, lícitas, explícitas y legítimas que justifiquen el tratamiento; e,
- III.- **Informada:** Que el titular tenga conocimiento del aviso de privacidad previo al tratamiento a que serán sometidos sus datos personales.

El principio de consentimiento como regla general deberá ir siempre ligada a las finalidades concretas del tratamiento de los datos personales y previo a su obtención es necesario que el titular conozca el aviso de privacidad.

En la obtención del consentimiento de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad declarada, se estará a lo dispuesto en los ordenamientos que resulten aplicables.

Artículo 16. El consentimiento podrá manifestarse de las siguientes formas:

- I.- **Expreso:** Cuando la voluntad del titular se manifieste verbalmente, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología. En el entorno digital podrá utilizarse la firma electrónica o cualquier mecanismo o procedimiento equivalente que permita identificar fehacientemente al titular, y a su vez, recabar su voluntad.
- II.- **Tácito:** Cuando habiéndose puesto a disposición del titular el aviso de privacidad, éste no manifieste su voluntad en sentido contrario.

Por regla general será válido el consentimiento tácito, salvo que las disposiciones normativas aplicables exijan que la voluntad del titular se manifieste expresamente.

Tratándose de datos personales sensibles el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica o cualquier mecanismo de autenticación que al efecto se establezca, salvo en los casos previstos en el Artículo 19 de este reglamento.

Artículo 17. Para la obtención del consentimiento expreso, el responsable deberá facilitar al titular un medio sencillo y gratuito a través del cual pueda manifestar su voluntad.

Artículo 18. Se entenderá que el responsable obtiene los datos personales de forma:

- a).- **Directa:** A través del titular cuando éste los proporciona personalmente o por algún medio que permita su entrega directa al responsable de manera enunciativa más no limitativa, medios electrónicos, ópticos, sonoros, visuales, vía telefónica, Internet

o cualquier otra tecnología o medio.

- b).- Indirecta:** Cuando el titular no los haya proporcionado personalmente o de manera directa al responsable, esto es a través de una transferencia.

Para el caso de la obtención indirecta de datos personales se deberá poner a disposición del titular de los datos personales el aviso de privacidad mediante correo postal o correo electrónico; el responsable podrá asumir que cuenta con consentimiento tácito una vez que haya transcurrido cinco días hábiles y el titular no haya manifestado su negativa para el tratamiento de datos personales en materia de datos personales sensibles se requiere el consentimiento expreso y por escrito.

Artículo 19. El responsable no estará obligado a recabar el consentimiento del titular para el tratamiento de sus datos personales en los siguientes casos:

- I.- Cuando una ley así lo disponga, debiendo dichos supuestos ser acordes con las bases, principios y disposiciones establecidos en la Ley General y el presente reglamento en ningún caso podrán contravenirla;
- II.- Cuando las transferencias que se realicen entre responsables, sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;
- III.- Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;
- IV.- Para el reconocimiento o defensa de derechos del titular ante autoridad competente;
- V.- Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;
- VI.- Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;
- VII.- Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico, 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.- Cuando el titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley en materia.

Artículo 20. El responsable deberá adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos, que motivaron su tratamiento implicando así el principio de calidad.

Artículo 21. Se presume que se cumple con la calidad en los datos personales cuando éstos son proporcionados directamente por el titular y hasta que éste no manifieste y acredite lo contrario.

Cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a

las disposiciones que resulten aplicables, deberán ser suprimidos, previo bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos.

Los plazos de conservación de los datos personales no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron su tratamiento, y deberán atender a las disposiciones aplicables en la materia de que se trate y considerar los aspectos administrativos, contables, fiscales, jurídicos e históricos de los datos personales.

Artículo 22. El responsable deberá establecer y documentar los procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales en su posesión, en los cuales se incluyan los periodos de conservación de los mismos.

En los procedimientos a que se refiere el párrafo anterior, el responsable deberá incluir mecanismos que le permitan cumplir con los plazos fijados para la supresión de los datos personales, así como para realizar una revisión periódica sobre la necesidad de conservar datos personales.

Artículo 23. El responsable sólo deberá tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento; entendiéndose con ello a la proporcionalidad de los datos personales tratados sean los mínimos necesarios para lograr la finalidad acorde a las facultades y atribuciones conferidas por disposición normativa.

Artículo 24. El principio de información, implica que el responsable deberá informar al titular a través del aviso de privacidad la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.

En este sentido, todo responsable que trate datos personales, sin importar la actividad que realice, requiere elaborar y poner a disposición los avisos de privacidad que correspondan a los tratamientos que lleven a cabo; por lo que deberán tener el número de avisos que resulten necesarios.

Artículo 25. Por regla general, el aviso de privacidad deberá ser difundido por los medios electrónicos y físicos, medios verbales o cualquier otra tecnología, para que el aviso de privacidad cumpla de manera eficiente con su función de informar, deberá estar redactado y estructurado de manera clara y sencilla.

Cuando resulte imposible dar a conocer al titular el aviso de privacidad, de manera directa o ello exija esfuerzos desproporcionados, el responsable podrá instrumentar medidas compensatorias de comunicación masiva de acuerdo con los criterios que para tal efecto emita el Sistema Nacional.

Artículo 26. El aviso de privacidad a que se refiere el artículo 4, fracción II, se pondrá a disposición del titular en dos modalidades: simplificado e integral; en un lugar visible, accesible y gratuito.

Artículo 27. El aviso simplificado deberá contener la siguiente información:

- I.- La denominación del responsable;
- II.- Las finalidades del tratamiento para las cuales se obtienen los datos personales,

distinguiendo aquéllas que requieran el consentimiento del titular;

- III.- Cuando se realicen transferencias de datos personales que requieran consentimiento, se deberá informar:
 - a).- Las autoridades, poderes, entidades, órganos y organismos gubernamentales del Municipio de Benito Juárez y del Estado de Quintana Roo y las personas físicas o morales a las que se transfieren los datos personales; y,
 - b).- Las finalidades de estas transferencias;
- IV.- Los mecanismos y medios disponibles para que el titular, en su caso, pueda manifestar su negativa para el tratamiento de sus datos personales, para finalidades y transferencias de datos personales que requieren el consentimiento del titular; y,
- V.- El sitio donde se podrá consultar el aviso de privacidad integral.

Los mecanismos y medios a los que se refiere la fracción IV, de este artículo, deberán estar disponibles para que el titular pueda manifestar su negativa al tratamiento de sus datos personales para las finalidades o transferencias que requieran el consentimiento del titular, previo a que ocurra dicho tratamiento.

La puesta a disposición del aviso de privacidad al que se refiere este artículo no exime al responsable de su obligación de proveer los mecanismos para que el titular pueda conocer el contenido del aviso de privacidad al que refiere el artículo 28 de este reglamento.

Artículo 28. El aviso de privacidad integral, además de lo dispuesto en las fracciones del artículo 27 de este reglamento, deberá contener, al menos, la siguiente información:

- I.- El 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:
 - a).- El tratamiento de datos personales; y,
 - b).- Las transferencias de datos personales que, en su caso, efectúe con autoridades, poderes, entidades, órganos y organismos gubernamentales de los tres órdenes de gobierno y las personas físicas o morales de carácter privado;
- IV.- Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requiere el consentimiento del titular;
- V.- Los mecanismos, medios y procedimientos disponibles para ejercer los derechos ARCO;
- VI.- El domicilio de la Unidad de Transparencia; y,
- VII.- Los medios a través de los cuales el responsable comunicará a los titulares los cambios del aviso de privacidad.

Artículo 29. Por regla general el aviso de privacidad se pone a disposición del titular previo al tratamiento de los datos personales y de la obtención de los datos personales

específicamente en los siguientes momentos:

- I.- Cuando los datos personales se obtienen de manera directa del titular previo a la obtención de los mismos, y;
- II.- Cuando los datos personales se obtienen de manera indirecta del titular previo al uso o aprovechamiento de estos.

Artículo 30. El principio de responsabilidad, establece la obligación de los responsables de velar por el cumplimiento de los demás principios y adoptar las medidas necesarias para su aplicación debiendo implementar los mecanismos previstos en el artículo 31 del presente reglamento para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en este ordenamiento; y rendir cuentas sobre el tratamiento de datos personales en su posesión al titular, al Instituto, y a la Unidad de Transparencia.

Se deberá observar para tal efecto la legislación aplicable en la materia, podrá valerse de estándares o mejores prácticas nacionales o internacionales para tales fines, en lo que no se contraponga con la normativa mexicana. Lo anterior, aplicará aún y cuando los datos personales sean tratados por parte de un encargado, así como al momento de realizar transferencias de datos personales.

Artículo 31. El responsable para cumplir con el principio de responsabilidad establecido en el presente reglamento deberá adoptar por lo menos los siguientes mecanismos:

- I.- Destinar recursos autorizados para la instrumentación de programas y políticas de protección de datos personales;
- II.- Elaborar políticas y programas de protección de datos personales obligatorios y exigibles al interior de la organización del responsable;
- III.- Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales;
- IV.- Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran;
- V.- Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorias, para comprobar el cumplimiento de las políticas de protección de datos personales;
- VI.- Establecer procedimientos para recibir y responder dudas y quejas de los titulares;
- VII.- Diseñar, desarrollar e implementar sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en el presente reglamento y las demás disposiciones normativas que resulten aplicables; y,
- VIII.- Garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, cumplan por defecto con las obligaciones previstas en la presente Ley y las demás que resulten aplicables en la materia.

El responsable deberá revisar las políticas y procedimientos de control a que se refiere la

fracción V del presente artículo, al menos cada dos años y actualizarlas cuando el tratamiento de datos personales sufra modificaciones sustanciales.

CAPÍTULO II De los Deberes

Artículo 32. Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

Artículo 33. Las medidas de seguridad adoptadas por el responsable deberán considerar:

- I.- El riesgo inherente a los datos personales tratados;
- II.- La sensibilidad de los datos personales tratados;
- III.- El desarrollo tecnológico;
- IV.- Las posibles consecuencias de una vulneración para los titulares;
- V.- Las transferencias de datos personales que se realicen;
- VI.- El número de titulares;
- VII.- Las vulneraciones previas ocurridas en los sistemas de tratamiento; y,
- VIII.- El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.

Artículo 34. Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:

- I.- Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión;
- II.- Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales;
- III.- Elaborar un inventario de datos personales y de los sistemas de tratamiento;
- IV.- El personal a cargo del responsable realizara un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros;
- V.- Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;
- VI.- Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de

gestión y tratamiento de los datos personales;

- VII.- Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales; y,
- VIII.- Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

Artículo 35. En el diseño e implementación de las políticas internas para la gestión y tratamiento de los datos personales, el responsable deberá aplicar por lo menos lo siguiente:

- I.- Garantizar que se valida la confidencialidad, integridad y disponibilidad de los datos personales;
- II.- La restauración, disponibilidad y el acceso a los datos personales de manera oportuna en caso de un incidente físico o técnico;
- III.- Las medidas correctivas en caso de identificar una vulneración o incidente en los tratamientos de datos personales;
- IV.- Establecer un proceso de evaluación periódica respecto a las políticas, procedimientos y planes de seguridad establecidos, a efecto de mantener su eficacia;
- V.- Los controles para garantizar que únicamente el personal autorizado podrá tener acceso a los datos personales para las finalidades concretas, lícita, explícitas y legítimas que originaron su tratamiento;
- VI.- Las medidas preventivas para proteger los datos personales contra su destrucción accidental o ilícita, su pérdida o alteración y el almacenamiento, tratamiento, acceso o transferencias no autorizadas o acciones que contravengan las disposiciones del presente reglamento y demás que resulten aplicables.

Artículo 36. La seguridad de la información debe preservar la confidencialidad, integridad y disponibilidad de los datos personales, entendiendo por estas obligaciones lo siguiente:

- a).- **Integridad:** Salvaguardar la exactitud y completitud de la información, así como evitar las modificaciones no autorizadas o accidental de la misma.
- b).- **Confidencialidad:** Propiedad de la información para no estar a disposición o ser revelada a personas no autorizadas.
- c).- **Disponibilidad:** Propiedad de un dato para ser accesible y utilizable, prevenir interrupciones no autorizadas.

Artículo 37. Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión. Se entenderá por sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, de conformidad con lo previsto en el presente reglamento y las demás disposiciones que le resulten aplicables en la materia.

Artículo 38. De manera particular, el responsable deberá elaborar un documento de

seguridad que contenga, al menos, lo siguiente:

- I.- El inventario de datos personales y de los sistemas de tratamiento;
- II.- Las funciones y obligaciones de las personas que traten datos personales;
- III.- El análisis de riesgos;
- IV.- El análisis de brecha;
- V.- El plan de trabajo;
- VI.- Los mecanismos de monitoreo y revisión de las medidas de seguridad; y,
- VII.- El programa general de capacitación.

Artículo 39. El responsable deberá actualizar el documento de seguridad cuando ocurran los siguientes eventos:

- I.- Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;
- II.- Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;
- III.- Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida; e,
- IV.- Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

Artículo 40. En caso de que ocurra una vulneración a la seguridad, el responsable deberá analizar las causas por las cuales se presentó e implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales si fuese el caso a efecto de evitar que la vulneración se repita.

Artículo 41. Además de las que señalen las leyes respectivas y la normatividad aplicable, se consideran como vulnerables de seguridad, en cualquier fase del tratamiento de datos, al menos, las siguientes:

- I.- La pérdida o destrucción no autorizada;
- II.- El robo, extravío o copia no autorizada;
- III.- El uso, acceso o tratamiento no autorizado; o,
- IV.- El daño, la alteración o modificación no autorizada.

Artículo 42. El responsable deberá llevar una bitácora de las vulnerabilidades a la seguridad ocurridas en la que se describa ésta, la fecha en la que ocurrió, el motivo de la misma y las acciones correctivas implementadas de forma inmediata y definitiva.

Artículo 43. El responsable deberá informar sin dilación alguna al titular y a la Unidad de Transparencia, las vulneraciones de seguridad ocurridas que afecten de forma significativa los derechos patrimoniales o morales, en cuanto se confirme que ocurrió la vulneración y que el responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, a fin de que los titulares afectados

puedan tomar las medidas correspondientes para la defensa de sus derechos.

Artículo 44. El plazo máximo que el responsable tiene para notificar al titular y a la Unidad de Transparencia son 72 horas a partir de ocurrida la vulneración de datos personales, dicho plazo está computado en días naturales.

Las notificaciones realizadas por el responsable deberán comprender lo determinado en los artículos 67 y 68 de los lineamientos generales.

Una vez recibida una notificación de vulneración por parte del responsable, la Unidad de Transparencia deberá realizar las investigaciones previas a que haya lugar con la finalidad de allegarse de elementos que le permitan, en su caso, iniciar un procedimiento de verificación en términos de la ley general y demás disposición normativa aplicable.

Artículo 45. La Unidad de Transparencia podrá publicar directrices, recomendaciones y mejores prácticas en materia de seguridad de los datos personales, de acuerdo con los estándares nacionales e internacionales actuales en la materia.

TÍTULO TERCERO **Derechos de los Titulares y su ejercicio**

CAPÍTULO I **De los Derechos de Acceso, Rectificación, Cancelación y Oposición**

Artículo 46. En todo momento el titular o su representante podrán solicitar ante la Unidad de Transparencia, el acceso, rectificación, cancelación u oposición al tratamiento de los datos personales que le conciernen, de conformidad con lo establecido en el presente Título. El ejercicio de cualquiera de los derechos ARCO no es requisito previo, ni impide el ejercicio de otro.

Artículo 47. El titular tendrá derecho de acceder a sus datos personales que obren en posesión de los responsables, así como conocer la información relacionada con las condiciones, generalidades y particularidades de su tratamiento.

Artículo 48. El titular a través de la Unidad de Transparencia, tendrá derecho a solicitar a los responsables la rectificación o corrección de sus datos personales, cuando éstos resulten ser inexactos, incompletos o no se encuentren actualizados.

Artículo 49. El titular tendrá derecho a solicitar a través de la Unidad de Transparencia la cancelación de sus datos personales de los archivos, registros, expedientes y sistemas de los responsables, a fin de que los mismos ya no estén en su posesión y dejen de ser tratados por este último.

Artículo 50. El titular podrá oponerse al tratamiento de sus datos personales o exigir que se cese en el mismo, cuando:

- I.- Cuando siendo lícito el tratamiento, el mismo debe cesar para evitar que su persistencia cause un daño o perjuicio al titular, o
- II.- Sus datos personales sean objeto de un tratamiento automatizado, el cual le produzca efectos jurídicos no deseados o afecte de manera significativa sus

intereses, derechos o libertades, y estén destinados a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales y de género, fiabilidad o comportamiento.

CAPÍTULO II

Del Ejercicio de los Derechos de Acceso, Rectificación, Cancelación y Oposición.

Artículo 51. A efecto de brindar un mejor entendimiento se entiende por el acrónimo ARCO:

- a).- **Acceso:** Derecho del titular de solicitar el acceso a sus datos personales que se encuentren en las bases de datos, sistemas, archivos, registros o expedientes del responsable que los posee, almacene o utiliza, así como el tratamiento que se le da a sus datos.
- b).- **Ratificación:** Derecho del titular, de solicitar la corrección de sus datos al ser inexactos, incompletos o no estén actualizados.
- c).- **Cancelación:** Derecho del titular de solicitar se eliminen sus datos personales de los archivos, registros, expedientes, sistemas, base de datos del responsable; salvo que estén implícitos en una cuestión legal o para el cumplimiento de obligaciones.
- d).- **Oposición:** Derecho del titular de solicitar que sus datos personales no sean utilizados para determinada finalidad, salvo que estén implícitos en una cuestión legal o para el cumplimiento de obligaciones.

Artículo 52. La recepción y trámite de las solicitudes para el ejercicio de los derechos ARCO que se formulen a los responsables, mediante la Unidad de Transparencia, se sujetará al procedimiento establecido en el presente Título y demás disposiciones que resulten aplicables en la materia.

Artículo 53. Para el ejercicio de los derechos ARCO será necesario acreditar la identidad del titular, y en su caso, la identidad y personalidad con la que actúe el representante. El ejercicio de los derechos ARCO por persona distinta a su titular o a su representante, será posible, excepcionalmente, en aquellos supuestos previstos por disposición legal, o en su caso, por mandato judicial.

En el ejercicio de los derechos ARCO de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad de conformidad con las leyes civiles, se estará a las reglas de representación dispuestas en la misma legislación.

Tratándose de datos personales concernientes a personas fallecidas, la persona que acredite tener un interés jurídico, de conformidad con las leyes aplicables, podrá ejercer los derechos que les confiere el presente Capítulo, siempre que el titular de los derechos hubiere expresado fehacientemente su voluntad en tal sentido o que exista un mandato judicial para dicho efecto.

Artículo 54. En consideración a los lineamientos generales, para acreditar al titular o su representante, el responsable deberá solicitar:

- I.- El titular podrá acreditar su identidad a través de los siguientes medios:
 - a).- original y copia simple de identificación oficial; o,

- b).- Instrumentos electrónicos o mecanismos de autenticación permitidos por otras disposiciones legales que permitan su identificación fehacientemente.**
- II.- A través de su representante, éste deberá acreditar su identidad y personalidad presentando los siguientes medios:**
 - a).- original y copia simple de la identificación oficial del titular;**
 - b).- original y copia de la identificación oficial del representante; e,**
 - c).- Instrumento público, o carta poder simple firmada ante dos testigos, anexando copia simple de las identificaciones oficiales de quienes intervengan.**
- III.- En caso de menores de edad cuando sus padres ejercen la patria potestad, deberá acreditar su identidad y personalidad presentando los siguientes medios:**
 - a).- Original y copia del acta de nacimiento del menor; y,**
 - b).- Original y copia simple de la identificación oficial del padre o la madre que ejercerá el derecho.**
- IV.- En el caso de menores de edad que una persona distinta ejerza la patria potestad deberá acreditar su identidad y personalidad presentando los siguientes medios:**
 - a).- Original y copia del acta de nacimiento del menor;**
 - b).- Original y copia del documento legal que acredite la posesión de la patria potestad; y,**
 - c).- Original y copia simple de la identificación oficial de quien ejerce la patria potestad.**
- V.- Cuando los menores de edad están representados por un tutor deberá acreditar su identidad y personalidad presentando los siguientes medios:**
 - a).- Original y copia del acta de nacimiento del menor;**
 - b).- Original y copia del documento legal que acredite la tutela; y,**
 - c).- Original y copia simple de la identificación oficial de quien ejerce la tutela.**
- VI.- Para acreditar la identidad y personalidad de personas en estado de interdicción o incapacidad declarada por ley, deberán presentar:**
 - a).- Original y copia del documento legal de designación del tutor y/o representante legal; y,**
 - b).- Original y copia simple de la identificación oficial del tutor.**
- VII.- Para acreditar la identidad y personalidad de personas vinculadas a fallecidos, deberán presentar:**
 - a).- Original y copia del Acta de defunción;**
 - b).- Original y copia del documento que acredite el interés jurídico de quien pretende acreditar el derecho ARCO documento legal de designación del tutor; y,**
 - c).- Original y copia simple de la identificación oficial de quien solicita el derecho ARCO.**

Artículo 55. En la solicitud para el ejercicio de los derechos ARCO no podrán imponerse mayores requisitos que los siguientes:

- I.- El nombre del titular y su domicilio o cualquier otro medio para recibir notificaciones;
- II.- Los documentos que acrediten la identidad del titular y, en su caso, la personalidad e identidad de su representante;
- III.- La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos ARCO, salvo que se trate del derecho de acceso;
- IV.- La descripción del derecho ARCO que se pretende ejercer, o bien, lo que solicita el titular; y,
- V.- Cualquier otro elemento o documento que facilite la localización de los datos personales, en su caso.

Tratándose de una solicitud de acceso a datos personales, el titular deberá señalar la modalidad en la que prefiere que éstos se reproduzcan. El responsable deberá atender la solicitud en la modalidad requerida por el titular, salvo que exista una imposibilidad física o jurídica que lo limite a reproducir los datos personales en dicha modalidad, en este caso deberá ofrecer otras modalidades de entrega de los datos personales fundando y motivando dicha actuación.

Artículo 56. El ejercicio de los derechos ARCO deberá ser gratuito. Sólo podrán realizarse cobros para recuperar los costos de reproducción, certificación o envío, conforme a la normatividad que resulte aplicable.

Cuando el titular proporcione el medio magnético, electrónico o el mecanismo necesario para reproducir los datos personales, los mismos deberán ser entregados sin costo a éste.

La información deberá ser entregada sin costo, cuando implique la entrega de no más de veinte hojas simples. Podrán exceptuar el pago de reproducción y envío atendiendo a las circunstancias socioeconómicas del titular.

El responsable no podrá establecer para la presentación de las solicitudes del ejercicio de los derechos ARCO algún servicio o medio que implique un costo al titular.

Artículo 57. La Unidad de Transparencia establecerá procedimientos sencillos que permitan el ejercicio de los derechos ARCO, cuyo plazo de respuesta no deberá exceder de veinte días contados a partir del día siguiente a la recepción de la solicitud.

El plazo referido en el párrafo anterior podrá ser ampliado por una sola vez hasta por diez días cuando así lo justifiquen las circunstancias, siempre y cuando, se le notifique al titular dentro del plazo de respuesta.

En caso de resultar procedente el ejercicio de los derechos ARCO, el responsable deberá hacerlo efectivo en un plazo que no podrá exceder de quince días contados a partir del día siguiente en que se haya notificado la respuesta al titular.

Artículo 58. En el caso de que la solicitud de protección de datos no satisfaga alguno de los requisitos a que se refiere el artículo 55 de este reglamento, y la Unidad de Transparencia no cuente con elementos para subsanarla, se prevendrá al titular de los datos dentro de los cinco días siguientes a la presentación de la solicitud de ejercicio de los derechos ARCO, por una sola ocasión, para que subsane las omisiones dentro de un plazo de diez días

contados a partir del día siguiente al de la notificación.

La prevención tendrá el efecto de interrumpir el plazo que tiene el responsable, para resolver la solicitud de ejercicio de los derechos ARCO, por lo que comenzará a computarse al día siguiente del desahogo por parte del titular.

Transcurrido el plazo sin desahogar la prevención se tendrá por no presentada la solicitud de ejercicio de los derechos ARCO.

Artículo 59. Con relación a una solicitud de cancelación, el titular deberá señalar las causas que lo motivan a solicitar la supresión de sus datos personales en los archivos, registros o bases de datos del responsable.

Artículo 60. Con relación a una solicitud de oposición, el titular deberá manifestar las causas legítimas o la situación específica que lo llevan a solicitar el cese en el tratamiento, así como el daño o perjuicio que le causaría la persistencia del tratamiento, o en su caso, las finalidades específicas respecto de las cuales requiere ejercer el derecho de oposición.

Artículo 61. El titular, por sí mismo o por medio de su representante podrá presentar las solicitudes para el ejercicio de los derechos ARCO, a través de escrito libre, formatos, medios electrónicos o cualquier otro medio que establezca Plataforma Nacional, el Instituto o la Unidad de Transparencia.

Si la solicitud para el ejercicio de los derechos ARCO es presentada ante un área y/o unidad administrativa distinta a la Unidad de Transparencia, aquella tendrá la obligación de indicar al titular la ubicación física de la Unidad de Transparencia.

La Unidad de Transparencia deberá dar trámite a toda solicitud para el ejercicio de los derechos ARCO que cumpla los requisitos determinados en el artículo 55 del presente reglamento y deberá entregar el acuse de recibo que corresponda.

La Unidad de Transparencia, podrá establecer formularios, sistemas y otros medios simplificados para facilitar a los titulares el ejercicio de los derechos ARCO; Los medios y procedimientos habilitados para atender las solicitudes para el ejercicio de los derechos ARCO deberán ser de fácil acceso con la mayor cobertura posible considerando el perfil de los titulares y la forma en que mantienen en contacto cotidiano o común con el responsable.

Artículo 62. Cuando el responsable no sea competente para atender la solicitud para el ejercicio de los derechos ARCO, deberá hacer del conocimiento del titular dicha solicitud dentro de los tres días siguientes a la presentación de la misma, y en caso de poder determinar, orientarlo hacia la autoridad competente.

En caso de que el responsable advierta que la solicitud para el ejercicio de los derechos ARCO corresponda a un derecho diferente de los previstos en la presente Ley, deberá reconducir la vía haciéndolo del conocimiento del titular; dejando a salvo los requisitos y plazos establecidos en la vía correcta conforme a la normatividad que resulte aplicable.

Artículo 63. Cuando se declare inexistencia de los datos personales, por parte del responsable en sus archivos, registros, sistemas o expediente, dicha declaración deberá constar en una resolución del Comité de Transparencia que confirme la inexistencia de los datos personales.

Dicha inexistencia deberá contar con los elementos mínimos que permita al titular tener la certeza de que se utilizó el criterio de búsqueda exhaustiva, así como señalar las circunstancias de tiempo, modo y lugar que generaron la inexistencia.

Artículo 64. Cuando las disposiciones aplicables a determinados tratamientos de datos personales establezcan un trámite o procedimiento específico para solicitar el ejercicio de los derechos ARCO, el responsable y/o la Unidad de Transparencia deberá informar al titular sobre la existencia del mismo, en un plazo no mayor a cinco días siguientes a la presentación de la solicitud para el ejercicio de los derechos ARCO, a efecto de que este último decida si ejerce sus derechos a través del trámite específico.

Artículo 65. Las únicas causas en las que el ejercicio de los derechos ARCO no será procedente son:

- I. Cuando el titular o su representante no estén debidamente acreditados para ello;
- II. Cuando los datos personales no se encuentren en posesión del responsable;
- III. Cuando exista un impedimento legal;
- IV. Cuando se lesionen los derechos de un tercero;
- V. Cuando se obstaculicen actuaciones judiciales o administrativas;
- VI. Cuando exista una resolución de autoridad competente que restrinja el acceso a los datos personales o no permita la rectificación, cancelación u oposición de los mismos;
- VII. Cuando la cancelación u oposición haya sido previamente realizada;
- VIII. Cuando el responsable no sea competente;
- IX. Cuando sean necesarios para proteger intereses jurídicamente tutelados del titular;
- X. Cuando sean necesario para dar cumplimiento a obligaciones legalmente adquiridas por el titular;
- XI. Cuando en función de sus atribuciones legales el uso cotidiano, resguardo y manejo sean necesarios y proporcionales para mantener la integridad, estabilidad y permanencia del Estado Mexicano; o,
- XII. Cuando los datos personales sean parte de la información que las unidades administrativas sujetas a la regulación y supervisión financiera del sujeto obligado haya proporcionado a este, en cumplimiento a requerimientos de dicha información sobre sus operaciones, organización y actividades.

En todos los casos anteriores, la Unidad de Transparencia deberá informar al titular el motivo de su determinación, en el plazo de hasta veinte días de conformidad con lo previsto en el primer párrafo del artículo 56 del presente reglamento y demás disposiciones aplicables, y por el mismo medio en que se llevó a cabo la solicitud, acompañando en su caso, las pruebas que resulten pertinentes.

En las respuestas a las solicitudes para el ejercicio de los derechos ARCO, la Unidad de Transparencia deberán informar al solicitante del derecho y plazo que tienen para promover el recurso de revisión.

Artículo 66. Contra la negativa de dar trámite a toda solicitud para el ejercicio de los

derechos ARCO o por falta de respuesta del responsable, procederá la interposición del recurso de revisión a que se refiere el artículo 113 del presente reglamento.

Artículo 67. En caso de que los documentos sobre los que se pretende ejercer el derecho de acceso a datos personales contenga información de acceso restringido en términos de la Ley General de Transparencia, la Ley de Transparencia y el Reglamento de Transparencia y no concierna al particular, la Unidad de Transparencia a través del responsable proporcionará los datos personales del titular y la información que tenga el carácter de pública, eliminando las partes o secciones clasificadas como reservadas o confidenciales, a excepción de que sobre estas últimas medie la autorización expresa de su titular. En tales casos, deberá señalarse qué partes o secciones fueron eliminadas conforme a la determinación del Comité de Transparencia.

Artículo 68. La Unidad de Transparencia debe de orientar en forma sencilla y comprensible a toda persona, aun cuando no sepa leer ni escribir, sobre los trámites y procedimientos que deben efectuarse para ejercer sus derechos de acceso, rectificación, cancelación u oposición de sus datos personales, las autoridades o instancias competentes, la forma de realizarlos, la manera de llenar los formularios que se requieran, así como de las instancias ante las que se puede acudir a solicitar orientación o formular quejas, consultas o reclamos sobre la prestación del servicio.

Artículo 69. Los medios por los cuales el solicitante podrá recibir notificaciones serán: correo electrónico, a través del sistema electrónico o en la Unidad de Transparencia.

En el caso de que el solicitante no señale domicilio o algún medio para oír y recibir notificaciones, el acuerdo o notificación se dará a conocer por lista que se fije en los estrados de la Unidad de Transparencia.

Artículo 70. En caso de que la solicitud presentada no corresponda al ejercicio de los derechos ARCO, la Unidad de Transparencia deberá notificarlo dentro del plazo de cinco días hábiles al solicitante y, en su caso, orientarlo para que presente una solicitud de acceso a información pública y/o en su defecto canalizarlo a la unidad administrativa competente.

En caso de que mediante una misma solicitud se pretenda ejercer derechos ARCO y acceder a información pública se atenderá la solicitud conforme a los plazos y términos del presente reglamento por lo que respecta a las peticiones en materia de datos personales. En la respuesta se deberá orientar a titular sobre la forma en la que podrá ejercer su derecho a la información pública.

Si el responsable es competente para atender parcialmente la solicitud para el ejercicio de los derechos ARCO, deberá dar respuesta conforme a su competencia.

CAPÍTULO III

De la Portabilidad de los Datos

Artículo 71. Cuando se traten de datos personales por vía electrónica en un formato estructurado y comúnmente utilizado, el titular tendrá derecho a obtener del responsable una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos.

Cuando el titular haya facilitado los datos personales y el tratamiento se base en el consentimiento o en un contrato, tendrá derecho a transmitir dichos datos personales y cualquier otra información que haya facilitado y que se conserve en un sistema en un formato electrónico comúnmente utilizado, sin impedimentos por parte del responsable del tratamiento de quien se retiren los datos personales.

Los responsables deberán observar y atender los parámetros a considerar para determinar los supuestos en los que se está en presencia de un formato estructurado y comúnmente utilizado, así como las normas técnicas, modalidades y procedimientos para la transferencia de datos personales, en términos de los lineamientos que emita el Sistema Nacional.

TÍTULO CUARTO **Relación del Responsable y Encargado**

CAPÍTULO ÚNICO **Del Responsable y Encargado**

Artículo 72. El encargado deberá realizar las actividades de tratamiento de los datos personales sin ostentar poder alguno de decisión sobre el alcance y contenido del mismo, así como limitar sus actuaciones a los términos fijados por el responsable.

Artículo 73. La relación entre el responsable y el encargado deberá estar formalizada mediante contrato de cualquier otro instrumento jurídico que decida el responsable, de conformidad con la normativa que resulte aplicable, y que permita acreditar su existencia, alcance y contenido.

El responsable podrá libremente determinar las obligaciones que le correspondan y aquellas que llevará a cabo el encargado, de conformidad con las disposiciones previstas en el presente reglamento y demás normativa que resulte aplicable.

Artículo 74. En el contrato o instrumento jurídico que decida el responsable se deberá prever, al menos, las siguientes cláusulas generales relacionadas con los servicios que preste el encargado:

- I. Realizar el tratamiento de los datos personales conforme a las instrucciones del responsable;
- II. Abstenerse de tratar los datos personales para las finalidades distintas a las instruidas por el responsable;
- III. Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables;
- IV. Informar al responsable cuando ocurra una vulneración a los datos personales que trata a nombre y por instrucciones;
- V. Guardar confidencialidad respecto a los datos personales tratados;
- VI. Suprimir o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales;
- VII. Abstenerse de transferir los datos personales salvo en el caso de que el responsable

así lo determine, o la comunicación derive de una subordinación, o por mandato expreso de la autoridad competente;

- VIII. Permitir al responsable y/o a la Unidad de Transparencia realizar inspecciones y verificaciones en el lugar o establecimiento donde se lleva a cabo el tratamiento de los datos personales; y,
- IX. Generar, actualizar y conservar la documentación necesaria que le permita acreditar el cumplimiento de sus obligaciones.

Los acuerdos entre el responsable y el encargado relacionados con el tratamiento de datos personales no deberán contravenir la Ley General, la Ley, el presente reglamento y las demás disposiciones aplicables, así como lo establecido en el aviso de privacidad correspondiente.

Artículo 75. Cuando el encargado incumpla las instrucciones del responsable y decida por sí mismo sobre la naturaleza, alcance, finalidades, medios u otras acciones relacionadas con el tratamiento de los datos personales, asumirá el carácter de responsable conforme a la legislación en la materia que le resulte aplicable.

Artículo 76. El encargado podrá, a su vez, subcontratar servicios que impliquen el tratamiento de datos personales por cuenta del responsable, siempre y cuando medie la autorización expresa de este último. El subcontratado asumirá el carácter de encargado en los términos del presente reglamento y demás disposiciones que resulten aplicables en la materia.

Cuando el contrato o el instrumento jurídico mediante el cual se haya formalizado la relación entre el responsable y el encargado, prevea que este último pueda llevar a cabo a su vez las subcontrataciones de servicios, la autorización en la que refiere el párrafo anterior se entenderá como otorgada a través de lo estipulado en éstos.

Artículo 77. Una vez obtenida la autorización expresa del responsable, el encargado deberá formalizar la relación adquirida con el subcontratado a través de un contrato o cualquier otro instrumento jurídico que decida, de conformidad con la normatividad que le resulte aplicable, y permita acreditar la existencia, alcance y contenido de la prestación del servicio en términos de lo previsto en el presente Capítulo.

Artículo 78. El responsable podrá contratar o adherirse a servicios, aplicaciones e infraestructura en el cómputo, en la nube, y otras materias que impliquen el tratamiento de datos personales, siempre y cuando el proveedor externo garantice políticas de protección de datos personales equivalentes a los principios y deberes establecidos en el presente reglamento y demás disposiciones que resulten aplicables en la materia.

En su caso, el responsable deberá delimitar el tratamiento de los datos personales por parte del proveedor externo a través de cláusulas contractuales u otros instrumentos jurídicos.

Artículo 79. Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura de cómputo en la nube y otras materias, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, solo podrá utilizar aquellos en los que el proveedor:

- I. Cumpla, al menos, con lo siguiente:

- a).- Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece el presente reglamento y demás normatividad aplicable;
- b).- Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio;
- c).- Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que preste el servicio; y,
- d).- Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.

VI.- Cuenten con mecanismos, al menos, para:

- a).- Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta;
- b).- Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio;
- c).- Establecer y mantener medidas de seguridad para la protección de los datos personales sobre los que se preste el servicio;
- d).- Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable y que este último haya podido recuperarlos; e,
- e).- Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho responsable.

En cualquier caso, el responsable no podrá adherirse a servicios que no garanticen la debida protección de los datos personales, conforme al presente reglamento y demás disposiciones que resulten aplicables en la materia.

Artículo 80. Las remisiones nacionales e internacionales de datos personales que se realicen exclusivamente entre responsable y encargado no requerirán ser informadas al titular, ni contar con su consentimiento.

TÍTULO QUINTO **Comunicaciones de Datos Personales**

CAPÍTULO ÚNICO **De las Transferencias y Remisiones de Datos Personales**

Artículo 81. Toda transferencia de datos personales, sea esta nacional o internacional, se encuentra sujeta a consentimiento de su titular, salvo las excepciones previstas en los Artículos 19, 77 y 82 de este reglamento.

Artículo 82. Toda transferencia deberá formalizarse mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, de conformidad con la normatividad que le resulte aplicable al responsable, que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y

responsabilidades asumidas por las partes.

Lo dispuesto en el párrafo anterior, no será aplicable en lo siguiente:

- I.- Cuando la transferencia sea nacional y se realice entre responsables en virtud del cumplimiento de una disposición legal o en el ejercicio de atribuciones expresamente conferidas a éstos; o,
- II.- Cuando la transferencia sea internacional y se encuentre prevista en una ley o tratado suscrito y ratificado por México, o bien, se realice a petición de una autoridad extranjera u organismo internacional competente en su carácter de receptor, siempre y cuando las facultades entre el responsable transferente y receptor sean homólogas, o bien, las finalidades que motivan la transferencia sean análogas o compatibles respecto de aquellas que dieron origen al tratamiento de los datos personales que lleva a cabo el responsable transferente.

Artículo 83. Cuando la transferencia sea nacional, el receptor de los datos personales deberá tratar los datos personales, comprometiéndose a garantizar la confidencialidad y únicamente utilizará para los fines que fueron transferidos atendiendo a lo convenido en el aviso de privacidad que le será comunicado por el responsable transferente.

Artículo 84. El responsable sólo podrá transferir o hacer remisión de datos personales fuera del territorio nacional cuando el tercero receptor o el encargado se obliguen a proteger los datos personales conforme a los principios y deberes que establece el presente reglamento y las disposiciones que resulten aplicables en la materia.

Artículo 85. En toda transferencia de datos personales, el responsable deberá comunicar al receptor de los datos personales el aviso de privacidad conforme al cual se tratan los datos personales frente al titular.

Artículo 86. El responsable podrá realizar transferencias de datos personales sin necesidad de requerir el consentimiento del titular, en los siguientes supuestos:

- I.- Cuando la transferencia esté prevista en este reglamento u otras leyes, convenios o Tratados Internacionales suscritos y ratificados por México;
- II.- Cuando la transferencia se realice entre responsables, siempre y cuando los datos personales se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;
- III.- Cuando la transferencia sea legalmente exigida para la investigación y persecución de los delitos, así como la procuración o administración de justicia;
- IV.- Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho ante autoridad competente, siempre y cuando medie el requerimiento de esta última;
- V.- Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios, siempre y cuando dichos fines sean acreditados;
- VI.- Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular; y,

VII.- Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero.

La actualización de alguna de las excepciones previstas en este artículo, no exime al responsable de cumplir con las obligaciones previstas en el presente Capítulo que resulten aplicables.

Artículo 87. El responsable, en caso de considerarlo necesario, podrá solicitar la opinión de la Unidad de Transparencia respecto al cumplimiento de lo dispuesto por el presente reglamento en aquellas transferencias internacionales de datos personales que efectúe.

TÍTULO SEXTO

Acciones Preventivas en Materia de Protección de Datos Personales

CAPÍTULO I

De las Mejores Prácticas

Artículo 88. Para el cumplimiento de las obligaciones previstas en el presente reglamento, el responsable a través de la Unidad de Transparencia podrá desarrollar o adoptar, en lo individual o en acuerdo con otros responsables, encargados u organizaciones, esquemas de mejores prácticas que tengan por objeto:

- I.- Elevar el nivel de protección de los datos personales;
- II.- Armonizar el tratamiento de datos personales en un sector específico;
- III.- Facilitar el ejercicio de los derechos ARCO a los titulares;
- IV.- Facilitar las transferencias de datos personales;
- V.- Complementar las disposiciones previstas en la normatividad que resulte aplicable en materia de protección de datos personales; y,
- VI.- Demostrar ante la Unidad de Transparencia o, en su caso, los organismos garantes, el cumplimiento de la normatividad que resulte aplicable en materia de protección de datos personales.

Artículo 89. Todo esquema de mejores prácticas que busque la validación o reconocimiento por parte de la Unidad de Transparencia o, en su caso, de los organismos garantes deberá:

- I.- Cumplir con los parámetros que para tal efecto emita el Instituto Nacional y en su caso, el Instituto conforme a los criterios que fije el primero; y,
- II.- Ser notificado ante la Unidad de Transparencia de conformidad con el procedimiento establecido en los parámetros señalados en la fracción anterior, a fin de que sean evaluados y, en su caso, validados o reconocidos e inscritos en el registro al que refiere el último párrafo de este artículo.

La Unidad de Transparencia en coordinación con el Instituto y los Organismos garantes, según corresponda, emitirán las reglas de operación de los registros en los que se inscribirán aquellos esquemas de mejores prácticas validados o reconocidos.

Los Organismos garantes, podrán inscribir los esquemas de mejores prácticas que hayan reconocido o validado en el registro administrado por el Instituto, de acuerdo con las reglas que fije este último.

Artículo 90. Cuando el responsable pretenda poner en operación o modificar políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que a su juicio y de conformidad con este reglamento impliquen el tratamiento intensivo o relevante de datos personales, deberá realizar una evaluación de impacto en la protección de datos personales, y presentarla ante la Unidad de Transparencia, el cual podrá emitir recomendaciones no vinculantes especializadas en la materia de protección de datos personales.

El contenido de la evaluación de impacto a la protección de datos personales será determinado por el Sistema Nacional.

Artículo 91. Para efectos de este reglamento se considerará que se está en presencia de un tratamiento intensivo o relevante de datos personales, el cual amerita una evaluación de impacto a la protección de datos personales, en función de los siguientes factores:

- I.- El número de titulares;
- II.- El público objetivo;
- III.- Los riesgos inherentes a los datos personales a tratar;
- IV.- La sensibilidad de los datos personales;
- V.- Las transferencias de datos personales que se pretenden efectuar y su periodicidad, en su caso;
- VI.- El desarrollo de la tecnología utilizada, en su caso;
- VII.- La relevancia del tratamiento de datos personales en atención al impacto social o, económico del mismo, o bien, del interés público que se persigue; y,
- VIII.- Los demás factores que la Unidad de Transparencia determine.

Artículo 92. Los responsables que realicen una evaluación de impacto en la protección de datos personales, deberán presentarla ante la Unidad de Transparencia, treinta días anteriores a la fecha en que se pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología, ante la Unidad de Transparencia o los organismos garantes, según corresponda, a efecto de que emitan las recomendaciones no vinculantes correspondientes.

Artículo 93. La Unidad de Transparencia deberá emitir, de ser el caso recomendaciones no vinculantes sobre la evaluación de impacto en la protección de datos personales presentados por el responsable.

El plazo para la emisión de las recomendaciones a que se refiere el párrafo anterior será dentro de los treinta días siguientes contados a partir del día siguiente a la presentación.

Artículo 94. Cuando a juicio del responsable se puedan comprometer los efectos que se pretenden lograr con la posible puesta en operación o modificación de políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales o se trate de situaciones de emergencia o urgencia, no será necesario realizar la evaluación de impacto en la protección de datos personales.

Artículo 95. La Unidad de Transparencia podrá llevar a cabo evaluaciones de impacto a la privacidad de oficio respecto de aquellos programas, políticas públicas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que impliquen el tratamiento intensivo o relevante de datos personales, conforme a los lineamientos que para tal efecto emita.

CAPÍTULO II

De las Bases de Datos en Posesión de Instancias de Seguridad, Procuración y Administración de Justicia

Artículo 96. Los tratamientos de datos personales efectuados por responsables con atribuciones expresas en materia de seguridad, procuración y administración de justicia, además de cumplir con las obligaciones previstas en el presente reglamento, deberán acotarse a aquellos supuestos y categorías de datos personales que resulten estrictamente necesarios y relevantes para el ejercicio de sus funciones en dichas materias, así como establecer medidas de seguridad suficientes y necesarias para garantizar la integridad, disponibilidad y confidencialidad de los datos personales.

Artículo 97. Los responsables de las bases de datos a que se refiere este Capítulo, deberán establecer medidas de seguridad de nivel alto, para garantizar la integridad, disponibilidad y confidencialidad de la información, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

Artículo 98. El tratamiento de datos personales en materia de registros públicos, como el Registro Civil, se rige por lo dispuesto en sus leyes especiales. A pesar de lo anterior, los responsables respectivos deberán ajustar su normatividad y su gestión a los principios, garantías y deberes contenidos en este reglamento, en lo relativo a los servicios de consulta de sus bases de datos, la reproducción y transmisión por cualquier medio de la información que posean, así como por cuanto a las medidas de seguridad que deben adoptar.

Artículo 99. Las notificaciones por listas de acuerdos, estrados y boletines judiciales se ajustarán a lo dispuesto por las leyes especiales que les resulten aplicables, pero deberán adoptar los principios y garantías contenidos en esta Ley en la protección de datos personales.

TÍTULO SÉPTIMO

Responsables en Materia de Protección de Datos Personales en Posesión de los Sujetos Obligados

CAPÍTULO I

Comité de Transparencia

Artículo 100. El Comité de Transparencia como órgano colegiado, se integrará y funcionará conforme a lo dispuesto en el artículo 36 del Reglamento de transparencia y demás normatividad aplicable.

El Comité de Transparencia será la autoridad máxima en materia de protección de datos personales.

Artículo 101. Para los efectos del presente reglamento sin perjuicio de otras atribuciones que le sean conferidas en la normatividad que le resulte aplicable, el Comité de Transparencia tendrá las siguientes funciones:

- I.- Aprobar, supervisar y evaluar las políticas, programas, acciones y demás actividades que correspondan para el cumplimiento del presente reglamento y demás disposiciones que resulten aplicables en la materia;
- II.- Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, de conformidad con las disposiciones previstas en el presente reglamento y en aquellas disposiciones que resulten aplicables en la materia, en coordinación con el oficial de protección de datos personales, en su caso;
- III.- Instituir, en su caso, procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO;
- IV.- Confirmar, modificar o revocar las determinaciones en las que se declare la inexistencia de los datos personales, o se niegue por cualquier causa el ejercicio de alguno de los derechos ARCO;
- V.- Establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor observancia del presente reglamento y en aquellas disposiciones que resulten aplicables en la materia;
- VI.- Supervisar, en coordinación con las áreas o unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad;
- VII.- Dar seguimiento y cumplimiento a las resoluciones emitidas por el Instituto y el Instituto Nacional;
- VIII.- Establecer programas de capacitación y actualización para los servidores públicos en materia de protección de datos personales; y,
- IX.- Dar vista al órgano interno de control o instancia equivalente en aquellos casos en que tenga conocimiento, en el ejercicio de sus atribuciones, de una presunta irregularidad respecto de determinado tratamiento de datos personales; particularmente en casos relacionados con la declaración de inexistencia que realicen los responsables.

CAPÍTULO II

De la Unidad de Transparencia

Artículo 102. La Unidad de Transparencia, se integrará y funcionará conforme a lo dispuesto en la Ley de Transparencia, este reglamento y demás normativa aplicable, que tendrá las siguientes funciones:

- I.- Vigilar el cumplimiento del presente reglamento y demás disposiciones normativas que resulten aplicables;
- II.- Interpretar el presente reglamento en el ámbito administrativo;

- III.- Auxiliar y orientar al titular que lo requiera con relación al ejercicio del derecho a la protección de datos personales;
- IV.- Emitir disposiciones administrativas de carácter general para la debida aplicación y cumplimiento del presente reglamento;
- V.- Conocer y solventar las denuncias y/o recursos de revisión que interponga los titulares en los términos dispuestos en la Ley y demás disposiciones normativas aplicables a la materia;
- VI.- Promover y difundir el ejercicio del derecho a la protección de datos personales;
- VII.- Orientar y asesorar a los titulares en materia de protección de datos personales;
- VIII.- Coordinarse con las autoridades competentes para garantizar, en el ámbito de su respectiva competencia, condiciones de accesibilidad para que los titulares que pertenecen a grupos vulnerables puedan ejercer, en igualdad de circunstancias, su derecho a la protección de datos personales;
- IX.- Suscribir convenios de colaboración con el instituto;
- X.- Gestionar las solicitudes para el ejercicio de los derechos ARCO;
- XI.- Establecer mecanismos para asegurar que los datos personales solo se entreguen a su titular o su representante debidamente acreditados;
- XII.- Informar al titular o su representante el monto de los costos a cubrir por la reproducción y envío de los datos personales, con base en lo establecido en las disposiciones normativas aplicables;
- XIII.- Proponer al Comité de Transparencia los procedimientos internos que aseguren y fortalezcan mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO;
- XIV.- Aplicar instrumentos de evaluación de calidad sobre la gestión de las solicitudes para el ejercicio de los derechos ARCO;
- XV.- Asesorar a las áreas adscritas al responsable en materia de protección de datos personales; y,
- XVI.- Dar atención y seguimiento a los acuerdos emitidos por el Comité de Transparencia.

Los responsables promoverán acuerdos con instituciones públicas especializadas que pudieran auxiliarles a la recepción, trámite y entrega de las respuestas de información y solicitudes para el ejercicio de los derechos ARCO, en la lengua indígena, braille o cualquier formato accesible correspondiente, en forma más eficiente.

Artículo 103. El responsable procurará que las personas con algún tipo de discapacidad o grupos vulnerables, puedan ejercer, en igualdad de circunstancias su derecho a la protección de datos personales.

Artículo 104. En la designación del titular de dirección general de la Unidad de Transparencia, se sujetarán a lo dispuesto en la Ley de Transparencia y demás normatividad aplicable, considerando preferentemente la experiencia y especialización comprobable en materia de protección de datos personales.

Artículo 105. Cuando alguna unidad administrativa del responsable se negará a colaborar con la Unidad de Transparencia en la atención de las solicitudes para el ejercicio de los derechos ARCO, ésta dará aviso al Comité de Transparencia para que le ordene realizar sin demora las acciones conducentes.

Cuando persista la negativa de colaboración, la Unidad de Transparencia lo hará del conocimiento de la autoridad competente para que ésta inicie, en su caso, el procedimiento de responsabilidad respectivo.

CAPÍTULO III De los Enlaces

Artículo 106. El Titular de cada Sujeto Obligado y/o Unidad Administrativa designará cuando menos un Enlace de datos personales y un suplente quienes serán los responsables de coordinar con las Unidades Administrativas, para el cumplimiento de las disposiciones en materia de Protección de Datos Personales y demás que se establezcan en el presente Reglamento.

Las Unidades Administrativas a través de su Enlace, serán las responsables de elaborar las respuestas a las solicitudes de derechos ARCO, así como de proteger los datos personales acorde a las facultades y atribuciones de la unidad administrativa y su estructura orgánica.

Artículo 107. Son atribuciones de los Enlaces:

- I.- Ser el vínculo entre la Unidad de Transparencia y la Unidad Administrativa del Sujeto Obligado;
- II.- Recabar y actualizar las bases de datos personales que le sea proporcionada por cada Unidad Administrativa, acorde a facultades y atribuciones de ley;
- III.- Verificar y solicitar a todas las Unidades Administrativas del Sujeto Obligado, para que colaboren con los mecanismos de seguridad, deberes y principios determinados en el presente reglamento;
- IV.- Tramitar en tiempo y forma las Solicitudes de derecho de acceso, rectificación cancelación y oposición a la publicación de sus datos personales (ARCO) competencia del Sujeto Obligado, así como darles seguimiento hasta la entrega de la información correspondiente;
- V.- Proponer los procedimientos internos que contribuyan a la mayor eficiencia de las Unidades Administrativas del Sujeto Obligado en materia de protección de datos personales;
- VI.- Aplicar los procedimientos internos para garantizar el derecho a la protección de datos personales;
- VII.- Apoyar y asesorar a las Unidades Administrativas, en la elaboración de las versiones públicas correspondientes;
- VIII.- Observar y dar a conocer a las Unidades Administrativas el cumplimiento de los criterios y lineamientos en materia de información confidencial;
- IX.- Tener a su cargo y administrar las claves de los sistemas electrónicos para el resguardo de los datos personales;

- X.- Dar aviso a la Unidad de Transparencia cuando se vulneren datos personales en la unidad administrativa y/o exista un riesgo inherente; y,
- XI.- Las demás necesarias para el cumplimiento del presente reglamento y demás disposiciones aplicables a la materia.

Artículo 108. El titular de la Unidad Administrativa y/o Sujeto Obligado, propiciarán la permanencia del Enlace. Cuando un Enlace sea dado de baja, el Sujeto Obligado y/o Unidad Administrativa deberá informar a la Unidad de Transparencia, en un término no mayor a tres días hábiles, por oficio y remitiendo el soporte correspondiente.

Artículo 109. El Servidor Público que sea designado como Enlace deberá ser capacitado en temas de protección de datos personales, clasificación de información, por lo cual deberá contactar a la Unidad de Transparencia.

TÍTULO OCTAVO Órganos Garantes

CAPÍTULO I

Artículo 110. Para los efectos del presente reglamento y sin perjuicio de otras atribuciones que les sean conferidas en la Ley de Transparencia y demás normatividad que le resulte aplicable, el Instituto tendrá las atribuciones determinadas por el artículo 102 de la Ley.

CAPÍTULO II

De la Coordinación y Promoción del Derecho a la Protección de Datos Personales.

Artículo 111. La Unidad de Transparencia deberá colaborar con el Instituto y los organismos garantes, según corresponda, para capacitar y actualizar de forma permanente a todos sus servidores públicos en materia de protección de datos personales, a través de la impartición de cursos, seminarios, organización de foros, talleres y cualquier otra forma de enseñanza y entrenamiento que se considere pertinente.

Artículo 112. La Unidad de Transparencia, en el ámbito de sus respectivas competencias, deberá:

- I.- Promover que en las instituciones educativas de todos los niveles y modalidades el derecho a la protección de datos personales, así como una cultura sobre el ejercicio y respeto de éste;
- II.- Fomentar la creación de espacios de participación social y ciudadana que estimulen el intercambio de ideas entre la sociedad, los órganos de representación ciudadana y los responsables.

TÍTULO NOVENO Medio de Impugnación en Materia de Protección de Datos Personales en Posesión de los Sujetos Obligados

CAPÍTULO ÚNICO Disposiciones Comunes al Recurso de Revisión

Artículo 113. El titular o su representante podrán interponer recurso de revisión, a través de los siguientes medios:

- I.- Por escrito libre en el domicilio del Instituto o en las oficinas habilitadas que al efecto establezca;
- II.- Por correo certificado con acuse de recibo;
- III.- Por formatos que al efecto emita el Instituto;
- IV.- Por los medios electrónicos que para tal fin autoricen;
- V.- Cualquier otro medio que al efecto establezca el Instituto; y,
- VI.- Se presumirá que el titular acepta que las notificaciones le sean efectuadas por el mismo conducto que presentó su escrito, salvo que acredite haber señalado uno distinto para recibir notificaciones.

Artículo 114. Para la acreditación del titular o representante ante la interposición de un recurso de revisión deberá respetarse lo determinado en el Capítulo I, Título Noveno de la Ley.

Artículo 115. en el caso del recurso de revisión ante el instituto, procedimiento, conciliación y resoluciones entre el sujeto obligado, la Unidad de Transparencia y los responsables de las unidades administrativas deberán apegarse a lo determinado por los Capítulos II, III, IV y del Título Noveno de la Ley.

TÍTULO DÉCIMO **Facultad De Verificación Del Instituto**

CAPÍTULO ÚNICO

Del Procedimiento de Vigilancia y Verificación de Tratamientos de Datos Personales

Artículo 116. La Unidad de Transparencia tendrá la atribución de vigilar y verificar el cumplimiento de las disposiciones contenidas en el presente reglamento y demás ordenamientos que se deriven de ésta.

En el ejercicio de las funciones de vigilancia y verificación, la Unidad de Transparencia deberá guardar confidencialidad sobre la información a la que tenga acceso en virtud de la verificación correspondiente.

Artículo 117. La verificación podrá iniciarse:

- I.- De oficio cuando la Unidad de Transparencia cuente con indicios que le hagan presumir de manera fundada y motivada la existencia de violaciones al presente reglamento y demás normatividad que resulte aplicable; y,
- II.- Por denuncia del titular cuando considere que ha sido afectado por actos del responsable que puedan ser contrarios a lo dispuesto por el presente reglamento y demás normativa aplicable.

El derecho a presentar una denuncia precluye en el término de un año contado a partir del día siguiente en que se realicen los hechos u omisiones materia de la misma. Cuando los

hechos u omisiones sean de tracto sucesivo, el término empezará a contar a partir del día hábil siguiente al último hecho realizado.

La verificación no procederá en los supuestos de procedencia del recurso de revisión previsto en la Ley.

Artículo 118. Previo a la verificación respectiva, la Unidad de Transparencia podrá desarrollar investigaciones previas, con el fin de contar con elementos para fundar y motivar el acuerdo de inicio respectivo.

Para ello, la Unidad de Transparencia podrá requerir mediante mandamiento escrito debidamente fundado y motivado al denunciante, responsable o cualquier autoridad la exhibición de la información o documentación que estime necesaria.

El denunciante, responsable o cualquier autoridad deberán atender los requerimientos de información en los plazos y términos que el Instituto establezca.

Artículo 119. Si como resultado de las investigaciones previas, la Unidad de Transparencia no cuenta con elementos suficientes para dar inicio al procedimiento de verificación, emitirá el acuerdo que corresponda, sin que esto impida que el Instituto pueda iniciar dicho procedimiento en otro momento.

Artículo 120. Para la interposición de una denuncia y cumplimiento de resoluciones se deberá respetarse lo determinado en el título decimo y décimo primero de la Ley.

TÍTULO DÉCIMO PRIMERO Medidas de Apremio y Responsabilidades

CAPÍTULO I De las Medidas de Apremio

Artículo 121. Se podrá imponer las siguientes medidas de apremio para asegurar el cumplimiento del presente reglamento:

- I.- La amonestación pública; y,
- II.- La multa, equivalente a la cantidad de ciento cincuenta hasta mil quinientas veces el valor diario de la Unidad de Medida y Actualización.

El incumplimiento de los responsables será difundido en el portal de obligaciones de transparencia del Instituto y considerado en las evaluaciones que éste realice.

En caso de que el incumplimiento de las determinaciones del Instituto, implique la presunta comisión de un delito o una de las conductas señaladas en el Artículo 171 de la Ley, deberá denunciar los hechos ante la autoridad competente.

Las medidas de apremio de carácter económico no podrán ser cubiertas con recursos públicos.

Artículo 122. Si a pesar de la ejecución de las medidas de apremio previstas en el artículo 121 del presente reglamento, el responsable no cumple con la resolución, se requerirá el cumplimiento al superior jerárquico para que en el plazo de cinco días lo obligue a cumplir sin demora.

De persistir el incumplimiento, se aplicarán sobre el superior jerárquico las medidas de apremio establecidas en el artículo anterior. Transcurrido el plazo, sin que se haya dado cumplimiento, se dará vista a la autoridad competente en materia de responsabilidades.

Artículo 123. Las medidas de apremio a que se refiere el presente Capítulo, deberán ser aplicadas por el órgano de control, por sí mismos o con el apoyo de la autoridad competente, de conformidad con los procedimientos que establezcan las leyes respectivas.

Artículo 124. Las multas que fijen el Instituto se harán efectivas ante la Secretaría de Finanzas y Planeación del Gobierno del Estado, a través de los procedimientos que las leyes establezcan y el mecanismo implementado para ello.

Artículo 125. Para calificar las medidas de apremio establecidas en el presente Capítulo, el Órgano de control deberá considerar:

- I.- La gravedad de la falta del responsable, determinada por elementos tales como el daño causado, los indicios de intencionalidad, la duración del incumplimiento de las determinaciones del Instituto y de la Unidad de Transparencia, así como la afectación al ejercicio de sus atribuciones;
- II.- La condición económica del infractor; y,
- III.- La reincidencia.

Artículo 126. En caso de reincidencia, el órgano de control podrá imponer una multa equivalente hasta el doble de la que se hubiera determinado originalmente el propio Instituto. Se considerará reincidente al que habiendo incurrido en una infracción que haya sido sancionada, cometa otra del mismo tipo o naturaleza.

Artículo 127. Las medidas de apremio deberán aplicarse e implementarse en un plazo máximo de quince días, contados a partir de que sea notificada la medida de apremio al infractor.

CAPÍTULO II De las Sanciones

Artículo 128. Serán causas de sanción por incumplimiento de las obligaciones establecidas en la materia en el presente reglamento, las siguientes:

- I.- Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO;
- II.- Incumplir los plazos de atención previstos en el presente reglamento para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate;
- III.- Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;

- IV.-** Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos del presente reglamento;
- V.-** No contar con el Aviso de Privacidad, o bien, omitir en el mismo alguno de los elementos a que refieren los Artículos 26, 27 y 28 del presente reglamento y, según sea el caso, y demás disposiciones que resulten aplicables en la materia;
- VI.-** Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables. La sanción sólo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales;
- VII.-** Incumplir el deber de confidencialidad;
- VIII.-** No establecer las medidas de seguridad en los términos que establecen el presente reglamento;
- IX.-** Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad;
- X.-** Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en el presente reglamento;
- XI.-** Obstruir los actos de verificación de la autoridad;
- XII.-** Crear bases de datos personales en contravención a lo dispuesto por este reglamento;
- XIII.-** No acatar las resoluciones emitidas por el Instituto, y de la Unidad de Transparencia;
- XIV.-** Aplicar medidas compensatorias en contravención de los criterios que tales fines establezca el Sistema Nacional;
- XV.-** Declarar dolosamente la inexistencia de datos personales cuando éstos exista total o parcialmente en los archivos del responsable;
- XVI.-** No atender las medidas cautelares establecidas por el Instituto y la Unidad de Transparencia;
- XVII.-** Tratar los datos personales de manera que afecte o impida el ejercicio de los derechos fundamentales previstos en la Constitución Política de los Estados Unidos Mexicanos y la Constitución Política de Estado Libre y Soberano de Quintana Roo;
- XVIII.-** No presentar ante la Unidad de Transparencia la evaluación de impacto a la protección de datos personales en aquellos casos en que resulte obligatoria, de conformidad con lo previsto en la presente Ley y demás normativa aplicable;
- XIX.-** Realizar actos para intimidar o inhibir a los titulares en el ejercicio de los derechos ARCO;
- XX.-** Omitir la entrega del informe anual y demás informes a que se refiere el Artículo 62, fracción VII de la Ley de Transparencia, o bien, entregar el mismo de manera extemporánea; y,
- XXI.-** No cumplir con las disposiciones previstas en los artículos de la presente Ley.

Las causas de responsabilidad previstas en las fracciones I, II, IV, VI, X, XII, XV, XVI, XVIII, XIX, XX y XXI de este artículo, así como la reincidencia en las conductas previstas en el resto de las fracciones del mismo, serán consideradas como graves para efectos de su sanción administrativa.

Las sanciones de carácter económico no podrán ser cubiertas con recursos públicos.

Artículo 129. Para las conductas a que se refiere el artículo anterior se dará vista a la autoridad competente para que imponga o ejecute la sanción.

Artículo 130. Las responsabilidades que resulten de los procedimientos administrativos correspondientes, derivados de la violación a lo dispuesto por el Artículo 128, de este reglamento son independientes de las del orden civil, penal o de cualquier otro tipo que se puedan derivar de los mismos hechos.

Dichas responsabilidades se determinarán, en forma autónoma, a través de los procedimientos previstos en las leyes aplicables y las sanciones que, en su caso, se impongan por las autoridades competentes, también se ejecutarán de manera independiente.

Para tales efectos, el Instituto y/o la Unidad de Transparencia podrán denunciar ante las autoridades competentes cualquier acto u omisión violatoria de este reglamento y aportar las pruebas que consideren pertinentes, en los términos de las leyes aplicables.

Artículo 131. En aquellos casos en que el presunto infractor tenga la calidad de servidor público, la Unidad de Transparencia deberá remitir a la autoridad competente, junto con la denuncia correspondiente, un expediente en que se contengan todos los elementos que sustenten la presunta responsabilidad administrativa.

A efecto de sustanciar el procedimiento citado en este artículo la Unidad de Transparencia deberá elaborar una denuncia dirigida a la contraloría, órgano interno de control o su equivalente, con la descripción precisa de los actos u omisiones que, a su consideración, repercuten en la adecuada aplicación del presente reglamento y que pudieran constituir una posible responsabilidad.

Asimismo, deberá elaborar y remitir el expediente que contenga todos aquellos elementos de prueba que considere pertinentes para sustentar la existencia de la posible responsabilidad. Para tal efecto, se deberá acreditar el nexo causal existente entre los hechos controvertidos y las pruebas presentadas.

La denuncia y el expediente deberán remitirse a la contraloría conocimiento de los hechos, órgano interno de control o su equivalente dentro de los quince días siguientes a partir de que la Unidad de Transparencia tenga.

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

TRANSITORIOS

PRIMERO. - El presente reglamento entrará en vigor al día siguiente de su publicación en el Periódico Oficial del Gobierno del Estado de Quintana Roo.

SEGUNDO. - Queda derogada cualquier disposición que contravenga los principios, bases,

procedimientos y derechos reconocidos en el presente Reglamento de Protección de Datos Personales en posesión de Sujetos Obligados para el Municipio de Benito Juárez, Quintana Roo.

SEGUNDO. - Remítase el presente dictamen a la Secretaría General del Ayuntamiento, para los efectos legales conducentes.

Así lo acordaron por unanimidad de votos, los integrantes de las Comisiones Unidas de Gobierno, Régimen Interior y Anticorrupción y de Mejora Regulatoria, Transparencia, Protección de Datos Personales y Acceso a la Información Pública a los veinticinco días del mes de noviembre del año dos mil veintiuno.

FIRMAS DE LOS INTEGRANTES DE LA COMISIÓN

Que por lo antes expuesto y en atención al contenido del Dictamen de las Comisiones Unidas de Gobierno, Régimen Interior y Anticorrupción y de Mejora Regulatoria, Transparencia, Protección de Datos Personales y Acceso a la Información Pública, se tiene a bien someter a la aprobación de los integrantes del Honorable Ayuntamiento los siguientes:

PUNTOS DE ACUERDO

PRIMERO. - Se aprueba en sus términos el Dictamen de las Comisiones Unidas de Gobierno, Régimen Interior y Anticorrupción y de Mejora Regulatoria, Transparencia, Protección de Datos Personales y Acceso a la Información Pública, por el que se expide el Reglamento de Protección de Datos Personales en Posesión de Sujetos Obligados para el Municipio de Benito Juárez, Quintana Roo.

SEGUNDO. - Se aprueba expedir el Reglamento de Protección de Datos Personales en Posesión de Sujetos Obligados para el Municipio de Benito Juárez, Quintana Roo, en los términos del Dictamen de las Comisiones Unidas de Gobierno, Régimen Interior y Anticorrupción y de Mejora Regulatoria, Transparencia, Protección de Datos Personales y Acceso a la Información Pública.

TERCERO. - Publíquese el presente acuerdo en términos de ley.

LA CIUDADANA MAESTRA FLOR RUÍZ COSÍO, SECRETARIA GENERAL DEL AYUNTAMIENTO DEL MUNICIPIO DE BENITO JUÁREZ, QUINTANA ROO, CON FUNDAMENTO EN LO DISPUESTO EN EL ARTÍCULO 120 FRACCIÓN IX, DE LA LEY DE LOS MUNICIPIOS DEL ESTADO DE QUINTANA ROO, **REFRENDA** EL ACUERDO A QUE SE REFIERE EL **SEXTO** PUNTO DEL ORDEN DEL DÍA APROBADO EN LA **SEXTA SESIÓN ORDINARIA DEL HONORABLE AYUNTAMIENTO CONSTITUCIONAL DEL MUNICIPIO DE BENITO JUÁREZ, QUINTANA ROO, 2021-2024, DE FECHA 02 DICIEMBRE DEL 2021.**----

**MTRA. FLOR RUIZ COSIO
SECRETARIA GENERAL DEL AYUNTAMIENTO
DEL MUNICIPIO DE BENITO JUÁREZ, QUINTANA ROO**

LA CIUDADANA LICENCIADA MARÍA ELENA HERMELINDA LEZAMA ESPINOSA, PRESIDENTE MUNICIPAL, CON FUNDAMENTO EN LO DISPUESTO EN EL ARTÍCULO 90 FRACCIÓN VII, DE LA LEY DE LOS MUNICIPIOS DEL ESTADO DE QUINTANA ROO, **PROMULGA** EL ACUERDO A QUE SE REFIERE EL **SEXTO** PUNTO DEL ORDEN DEL DÍA APROBADO EN LA **SEXTA SESIÓN ORDINARIA DEL HONORABLE AYUNTAMIENTO CONSTITUCIONAL DEL MUNICIPIO DE BENITO JUÁREZ, QUINTANA ROO, 2021-2024**, DE FECHA **02 DE DICIEMBRE DEL 2021**. PUBLÍQUESE EN TÉRMINOS DE LEY. -----

LIC. MARÍA ELENA HERMELINDA LEZAMA ESPINOSA
PRESIDENTE MUNICIPAL
DEL MUNICIPIO DE BENITO JUÁREZ, QUINTANA ROO