

**Políticas internas para la
gestión y tratamiento de
los datos personales del
Consejo Nacional de
Evaluación de la Política de
Desarrollo Social
(CONEVAL)**

ÍNDICE

- I. Considerandos
- II. Objetivo
- III. Ámbito de aplicación
- IV. Principios generales para la protección de datos personales
- V. Políticas de operación
- VI. Políticas sobre Medidas de seguridad
- VII. Glosario
- VIII. Anexos

Políticas internas para la gestión y tratamiento de los datos personales en posesión del CONEVAL

I. Considerandos.

I.1 Que el artículo 16 segundo párrafo de la *Constitución Política de los Estados Unidos Mexicanos*, refiere que *“Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros”*.

I.2 Para reglamentar la disposición antes referida, con fecha 26 de enero de 2017, se publicó en el Diario Oficial de la Federación la *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados* (LGPDPPSO), la cual establece las bases, principios y procedimientos para garantizar el derecho humano que tiene toda persona a la protección de sus datos personales en posesión del sector público en los tres órdenes de gobierno. Con el objeto de desarrollar las disposiciones previstas en dicha Ley, con fecha 26 de enero de 2018 se publicó en el Diario Oficial de la Federación el Acuerdo mediante el cual se aprueban, *los Lineamientos Generales de Protección de Datos personales para el Sector Público* (Lineamientos Generales), emitidos por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Que el artículo 16 de la LGPDPPSO y 7 de los Lineamientos Generales señalan que los principios que se deben observar en el tratamiento de datos personales, son los de *licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad*. Asimismo, los artículos 30 y 31 de la LGPDPPSO y 46 y 47 de los Lineamientos Generales establecen el mecanismo que se deberá implementar para dar cumplimiento al principio de responsabilidad, el cual refiere a elaborar las políticas y programas de protección de datos personales, obligatorios y exigibles al interior de la organización, considerándose de manera enunciativa más no limitativa, el desarrollo tecnológico y las técnicas existentes la naturaleza, contexto, alcance, finalidades del tratamiento, atribuciones y facultades.

Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el artículo 33 de la LGPDPPSO dispone que el responsable deberá realizar, entre otras, la creación de 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. En tanto, el artículo 34 de la LGPDPPSO establece que las acciones relacionadas con las medidas de seguridad respecto al tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión.

Para la operación de este sistema de gestión, el Sujeto Obligado deberá contar con un Documento de Seguridad que deberá contener cuando menos los aspectos previstos en el artículo 35 de la LGPDPPSO, motivo por el cual se expiden las presentes Políticas como el instrumento que describe y da cuenta de manera general sobre los principios y procedimientos adoptados por el CONEVAL para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

II. Objetivo.

Establecer los elementos, principios y procedimientos de dirección, operación, seguridad y control que deberán observar las unidades administrativas del Consejo Nacional de Evaluación de la Política de Desarrollo Social (CONEVAL) en el ejercicio de las funciones y atribuciones que tienen conferidas, respecto de los procesos que impliquen el tratamiento de datos personales.

III. Ámbito de aplicación.

Las presentes políticas son de aplicación general y obligatoria para las y los servidores públicos del CONEVAL que en el ejercicio de sus funciones obtengan, usen, registren, organicen, conserven, elaboren, utilicen, comuniquen, difundan, almacenen, posean, manejen, aprovechen, divulguen, transfieran o dispongan de datos personales.

IV. Principios generales para la protección de datos personales.

Las personas servidoras públicas en el CONEVAL, deberán dar tratamiento a los Datos Personales, observando los principios siguientes:

Licitud: El responsable deberá tratar los datos personales que posea sujetándose a las atribuciones o facultades que la normatividad aplicable le confiera, respetando los derechos y libertades de los titulares. (*artículos 17 LGPDPPSO y 8 de los Lineamientos Generales*).

Finalidad: Todo tratamiento de datos personales que efectuó el responsable deberá estar contenido en las finalidades descritas en el aviso de privacidad que corresponda al proceso o gestión establecida por el CONEVAL, mismas que deberán estar relacionadas con las atribuciones que la normatividad aplicable les confiera. (*artículos 18 LGPDPPSO y 9 de los Lineamientos Generales*).

Lealtad: No se deberán obtener y tratar datos personales, a través de medios engañosos o fraudulentos, privilegiando la protección de los intereses del titular y respetar la confianza que ha depositado el Titular, respecto a que sus datos personales serán tratados conforme a lo señalado en el aviso de privacidad. (*artículos 19 LGPDPPSO y 11 de los Lineamientos Generales*).

Consentimiento: Previo al tratamiento de los datos personales se deberá contar con la aceptación del titular, ésta se podrá manifestar de forma expresa o tácita, con excepción de lo previsto en el artículo 22 de la LGPDPPSO. (*artículos 21 LGPDPPSO y 12 de los Lineamientos Generales*).

Calidad: Se deberán adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, con el fin de que no se altere la veracidad de éstos. (*artículos 23 LGPDPPSO y 23 de los Lineamientos Generales*).

Información: Se deberá informar al titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, con el fin de que pueda tomar decisiones informadas al respecto. (*artículos 26 LGPDPPSO y 26 de los Lineamientos Generales*).

Proporcionalidad: Sólo se deberá tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento. (*artículos 25 LGPDPPSO y 24 de los Lineamientos Generales*).

Responsabilidad: Se deberá implementar los mecanismos para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en la LGPDPPSO, entre otros, elaboración de políticas y programas de protección de datos personales, programas de capacitación y actualización, así como el desarrollo de sistemas o plataformas informáticas acordes al tratamiento. (*artículos 29 LGPDPPSO y 46 de los Lineamientos Generales*).

V. Políticas de operación.

Las personas servidoras públicas en el Coneval deberán dar tratamiento a los Datos Personales, observando lo siguiente:

Licitud.

- Las personas servidoras públicas del CONEVAL, deberán conocer la normatividad para el tratamiento de datos personales, en particular, la que regule las actividades y procesos que estén en el marco de sus atribuciones.
- Todos los procesos y actividades que consideren tratamiento de datos personales deberán contar con un aviso de privacidad y los datos personales involucrados deberán ser tratados conforme a las finalidades descritas en dicho aviso.
- En el tratamiento de datos personales de menores de edad, se deberá privilegiar el interés superior de las niñas, niños y adolescentes en términos de las disposiciones previstas en la Ley General de los Derechos de Niñas, Niños y Adolescentes.

Finalidad.

- Los datos personales sólo pueden ser tratados para cumplir con la finalidad o finalidades que hayan sido informadas al titular en el aviso de privacidad, por lo que estas deberán ser señaladas en el inventario de datos personales por unidad administrativa.

- Se deberá evitar que las finalidades que se describa en el aviso de privacidad sean inexactas, ambiguas o vagas, como “de manera enunciativa más no limitativa”, debiendo ser concretas, explícitas, lícitas y legítimas.
- Se deberá conservar los datos personales exclusivamente por el tiempo que sea necesario para llevar a cabo las finalidades que justificaron el tratamiento y para cumplir con aspectos legales, administrativos, contables, fiscales, jurídicos e históricos y el periodo de bloqueo. Temporalidad o plazo que se indicará en el Inventario de datos personales.

Lealtad

- Únicamente se podrán obtener los datos personales por los medios establecidos en el Inventario de datos personales que se elabora por unidad administrativa.
- Solo se recabarán datos personales para procesos institucionales a través de los mecanismos y herramientas que proporcione el CONEVAL.
- Respetar la confianza que ha depositado el Titular, respecto a que sus datos personales serán tratados conforme a lo señalado en el aviso de privacidad

Consentimiento

- En el momento previo a recabar los datos personales, se deberá poner a disposición del titular el aviso de privacidad, con el propósito de recabar el consentimiento tácito o expreso.
- En el caso de recabar datos personales sensibles, el consentimiento del titular para su tratamiento será expreso y por escrito a través de firma autógrafa, firma electrónica o cualquier otro mecanismo de autenticación, salvo en los casos establecidos en el artículo 22 de la LGPDPSO.
- En el caso de nuevas atribuciones del CONEVAL, en las cuales implique el tratamiento de Datos personales, la Unidad administrativa que le corresponda ejercer dichas atribuciones, deberá comunicar dicha situación a la Unidad de Transparencia, a efecto de determinar de manera conjunta con el área jurídica, el tipo de consentimiento que se requiere: tácito, expreso o expreso y por escrito, así como para la elaboración del aviso de privacidad en dos modalidades: simplificado e integral.
- Cuando se recaben datos personales sensibles, se 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, salvo en los casos previstos en el artículo 22 de la Ley.
- Cuando existan finalidades que requieran consentimiento del titular, deben implementarse medios y mecanismos para que el titular, de ser el caso, también pueda manifestar su negativa.
- El mecanismo para que el titular manifieste su negativa debe cumplir con los siguientes requisitos: estar disponible en ambos avisos; estar disponible al momento en que el titular consulta el aviso de privacidad; el mecanismo podrá estar representado por casillas u opciones de marcado en el propio aviso de privacidad, o bien, cualquier otro medio que determine pertinente, con la condición de que esté disponible al momento en que el titular

consulte el aviso de privacidad y permita que éste manifieste su negativa, previo al tratamiento de los datos o a la transferencia de los mismos.

- La Unidad de Transparencia establecerá, revisará y de ser el caso actualizará el protocolo para la atención de los derechos ARCO.
- La Unidad de Transparencia y/o el área designada para la mejora de la gestión supervisarán el establecimiento, actualización y el seguimiento de los avisos de privacidad simplificados e integrales, para cada proceso en el cual se realice el tratamiento de datos personales en el Coneval.
- En el caso del consentimiento de menores de edad se atenderá lo señalado en la Ley de niños, niñas y adolescentes y a la ley civil.

Calidad.

- Mediante los avisos de privacidad y el análisis del ciclo de vida de los datos personales mismo que se señala en el *Inventario de datos personales* (Inventario) la unidad administrativa propietaria del proceso en el cual se traten datos personales revisará e implementará, con el apoyo de la Unidad de Transparencia, las medidas necesarias para mantener los datos personales en posesión del CONEVAL exactos, correctos, completos y actualizados, con la finalidad de que no se altere su veracidad.
- No se dará tratamiento de datos personales parciales o incompletos que puedan inducir al error, en su caso, se deberán recabar los datos completos para reiniciar el tratamiento.

Proporcionalidad

- Las unidades administrativas responsables de los procesos o actividades descritas en el Inventario, deberán tratar sólo aquellos datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las cuales se recaban.
- La Unidad de Transparencia a través del inventario de datos personales de cada unidad administrativa analizará la pertinencia de la proporcionalidad de los datos que se recaben y realizará las sugerencias a las unidades administrativas.
- La Unidad de Transparencia a través del Inventario de datos personales de cada unidad administrativa analizará la pertinencia de que se recaben datos personales sensibles, y realizará las recomendaciones pertinentes a las unidades administrativas.
- Únicamente, se recabarán los Datos Personales pertinentes que permitan realizar la gestión del proceso que haya solicitado el Titular de los mismos.

Información

- Se deberá informar a los titulares de los datos personales, el propósito del tratamiento al que será sometida su información personal, lo que se materializa a través del aviso de privacidad.

- Cuando los datos se recaben de forma directa o personal, el aviso se realizará de manera previa al tratamiento.
- Cuando los datos se recaben de forma indirecta (a través de transferencias), el aviso se realizará al primer contacto, previo al tratamiento.
- Los responsables del proceso o actividad en la cual se traten datos personales deberán asegurarse de que el aviso de privacidad sea difundido en la página web del CONEVAL.
- En el caso de recabar los datos personales de forma directa y presencial, el aviso de privacidad deberá ubicarse en lugar visible y que facilite su consulta, con independencia de que se publique en la página web del CONEVAL.
- En el caso de que los datos personales se recaben a través de un formulario electrónico en la página web del CONEVAL los responsables del proceso deberán asegurarse de que el aviso se encuentre publicado en dicho sitio.
- Cuando se recaben datos personales vía correo electrónico, las Unidades administrativas deberá informar al titular el aviso de privacidad que corresponde al proceso determinado en el Inventario de datos personales, a través del mismo medio.
- Se deberá poner a disposición de los titulares un nuevo aviso de privacidad en los siguientes casos: cambie la identidad del responsable, se recaben nuevos datos personales, se definan nuevas finalidades y/o se realicen nuevas transferencias que requieran el consentimiento del titular.

Responsabilidad

- El personal que trate datos personales o que tenga acceso a los mismos, derivado de las funciones encomendadas, deberá guardar la confidencialidad, para lo cual, de considerarse procedente se deberá de suscribir carta de confidencialidad.
- El personal que tenga bajo su resguardo los expedientes que contengan datos personales y que sean solicitados por autoridades fiscalizadoras, deberán proporcionar la información en términos del artículo 22 fracción III de la LGPDPSO, y señalarle a las autoridades lo siguiente:

"La información que solicita es confidencial por contener datos personales; el CONEVAL, en su calidad de sujeto obligado es responsable de la protección de los datos personales y/o de la información confidencial que posea. En este sentido, se trasfiere la misma con fundamento en los artículos 117, fracción V, de la Ley Federal de Transparencia y Acceso a la Información Pública; 22 fracción III, 65, 66, fracción I, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; en razón de lo anterior, es responsabilidad de esa instancia fiscalizadora proteger y guardar la confidencialidad de la información entregada".

- El personal que tenga bajo su resguardo información que contengan datos personales y que sean solicitados por cualquiera de las unidades administrativas del CONEVAL en el ámbito de sus atribuciones, deberá incluir la siguiente leyenda al momento de su entrega:

“La información que se entrega contiene datos personales, por lo que en su calidad de receptor deberá garantizar su confidencialidad y únicamente la utilizará para los fines que fue entregado. Lo anterior de conformidad con el artículo 4, 6 y 31, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. El uso indebido de datos personales que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión, pudiera constituir un incumplimiento en sus obligaciones como servidor público.”

- El personal que reciba y/o tramite vía correo electrónico consultas, opiniones o cualquier comunicado que contengan datos personales, en el ámbito de sus atribuciones, deberá incluir la siguiente leyenda al momento de dar respuesta al titular de los datos:

“En atención a su solicitud, se le informa (lo que corresponda), asimismo que sus datos personales serán protegidos conforme a lo dispuesto por el artículo 42 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 9 y 16 de la Ley Federal de Transparencia y Acceso a la Información Pública.”

- Cuando se lleve a cabo tratamiento de datos personales a nombre y por cuenta del CONEVAL, se deberá formalizar un instrumento jurídico con el encargado (proveedor) a efecto de establecer derechos y obligaciones.
- El instrumento jurídico deberá estar validado y dictaminado por el área jurídica del CONEVAL y deberá establecer las cláusulas referentes a las medidas de seguridad y de tratamiento de datos personales para verificar su correspondencia con los requerimientos del CONEVAL, atendiendo a lo señalado en el artículo 59 de la LGPDPPSO.
- La Unidad administrativa que corresponda, deberá comunicar a la Unidad de Transparencia la información relativa al instrumento jurídico que se formalice para el tratamiento de Datos Personales, a efecto de registrar en la Bitácora la siguiente información:
 - ✓ Nombre del servicio
 - ✓ Proveedor (encargado)
 - ✓ No. de Contrato
 - ✓ Vigencia
 - ✓ Alcances en cuanto al tratamiento de datos personales
- Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura de computó en la nube, se deberá contemplar en el Anexo técnico lo establecido en los artículos 64 de la LGPDPPSO y 111 de los Lineamientos Generales.
- Cuando se realicen transferencias de datos personales se deberá mantener comunicación con la Unidad de Transparencia, para lo procedente.
- En caso de vulneraciones, la persona servidora pública responsable del proceso en cuestión deberá notificar a la Unidad de Transparencia para que se informe al titular de los datos, y al INAI, en un plazo máximo de setenta y dos horas, a partir de que confirme la ocurrencia de éstas y la persona servidora pública responsable haya empezado a tomar las

acciones encaminadas a detonar un proceso de mitigación de la afectación; para ello se deberá informar al menos lo siguiente:

- ✓ La naturaleza del incidente;
 - ✓ Los datos personales comprometidos;
 - ✓ Las recomendaciones al Titular acerca de las medidas que éste pueda adoptar para proteger sus intereses;
 - ✓ Las acciones correctivas realizadas de forma inmediata;
 - ✓ Los medios donde puede obtener más información al respecto;
 - ✓ La descripción de las circunstancias generales en torno a la vulneración recurrida, que ayuden al titular a entender el impacto del incidente.
- La Unidad de Transparencia deberá llevar una bitácora de vulneraciones a la seguridad, la cual debe contener: la fecha en la que ocurrió, el motivo de ésta y las acciones correctivas implementadas de forma inmediata y definitiva. La vulneración se registrará en el formato establecido por la Unidad de Transparencia y/o el área de mejora de la gestión, considerando lo señalado en el artículo 67 de los Lineamientos (fracciones I a la XII).
 - La Unidad de Transparencia y/o el área de mejora de la gestión establecerán el programa de capacitación que tenga como objetivo fortalecer y actualizar los conocimientos de las personas servidoras públicas en materia de protección de datos personales.

Verificación

- La Unidad de Transparencia coordinará las acciones encaminadas a la atención de procesos de verificación en el cumplimiento de las obligaciones señaladas por el INAI en materia de protección de datos personales.
- Las unidades administrativas del CONEVAL, atenderán los requerimientos y/u observaciones que sobre los procesos de su competencia señale el INAI derivado de los procesos de verificación.
- El CONEVAL podrá someterse de forma voluntaria a la realización de auditorías en términos de lo previsto en el artículo 151 de la LGPDPPSO.

VI. Políticas sobre Medidas de seguridad

a) Físicas

Las personas servidoras públicas del CONEVAL, deberán:

- Resguardar los expedientes en archiveros y gavetas bajo llave.
- Evitar reciclar documentos que contengan datos personales, así como verificar que no se utilicen hojas que puedan contener datos personales y/o información confidencial de la organización, ya que pudieran ser divulgados o expuestos y utilizados para finalidades distintas a las legítimas establecidas en el aviso de privacidad correspondiente.

- Evitar tirar documentos con datos personales sin triturar o destruir.
- No dejar documentos con datos personales en la fotocopadoras e impresoras.
- Mantener los escritorios limpios, cualquier documento o expediente debe estar resguardado, fuera de la vista, cuando no se esté utilizando.
- Proteger el acceso físico al lugar en el que se encuentra el medio de almacenamiento (cámaras de seguridad, guardias, acceso restringido con tarjeta de proximidad, entre otros).
- Bloquear los datos personales una vez agotado el periodo de conservación.
- Para el caso de las contrataciones de servicios en las que haya tratamiento de datos personales, atendiendo a la normatividad aplicable, la Unidad administrativa deberá gestionar la entrega de evidencia de la supresión de los datos personales, conforme a lo acordado en el instrumento jurídico que corresponda.

b) Administrativas.

- Cada unidad administrativa deberá integrar un Inventario de datos personales que considere la totalidad de los procesos que, en el ejercicio de sus atribuciones, competencias y funciones implique el tratamiento de datos personales.
- Cada unidad administrativa deberá identificar en los procesos en los cuales realice el tratamiento de datos personales, los riesgos y su valoración en relación con su impacto y probabilidad de ocurrencia.
- La Unidad de Transparencia, establecerá los procedimientos, guías o protocolos mediante los cuales se facilite a las unidades administrativas la elaboración de los inventarios de datos personales.
- La Unidad de Transparencia, integrará y administrará el *Inventario Institucional de datos personales*.
- Los inventarios de cada unidad administrativa se actualizarán periódicamente atendiendo a los cambios, mejoras, y deberán informarse para que se realice la actualización del Inventario Institucional de Datos Personales.
- La Unidad de Transparencia promoverá conjuntamente con las unidades administrativas, y el área de tecnologías de la información, la implementación de medidas de seguridad para la protección de datos personales.
- Las unidades administrativas que recaben los datos personales, así como la unidad de transparencia, tecnologías de la información y el área jurídica, en el ámbito de sus competencias, determinarán, los términos de los protocolos específicos para la transferencia de datos personales, así como las medidas de seguridad pertinentes.

- Los plazos de conservación de los documentos que contengan datos personales, establecidos en el inventario no deberán exceder aquéllos señalados en el *Catálogo de disposición documental vigente del CONEVAL*.

c) Técnicas

- Cada unidad administrativa deberá integrar un *Inventario de Sistemas* en el cual se registren aquellos que, en el ejercicio de sus atribuciones, competencias y funciones, se dé tratamiento a datos personales.
- En el ámbito de su competencia, la Unidad de Transparencia, las unidades administrativas y el área de Tecnología de la información (TIC's) establecerán los mecanismos de monitoreo y revisión de las medidas de seguridad.
- El área de TIC's identificará y mantendrá actualizado el inventario de infraestructuras esenciales y/o críticas, así como los mecanismos para garantizar su protección.
- La Unidad de Transparencia realizará monitoreos y establecerá conjuntamente con el área de TIC's una cadena de avisos en caso de vulnerabilidad a la seguridad de la información; asimismo, se harán periódicamente pruebas de intrusión.
- El área de TIC's realizará respaldos de manera regular y pruebas de recuperación.
- Se revisará de manera periódica la administración y asignación de contraseñas con el fin de apoyar a los administradores y usuarios de servicios de tecnología a reducir los impactos de los riesgos generados por el manejo y resguardo de la información.
- El personal del CONEVAL como usuario de los equipos informáticos, deberá tener un identificador único en el sistema al cuál se vincularán sus privilegios y accesos. Asimismo, cada usuario deberá ser responsable de guardar en secreto la(s) contraseña(s) y/o mecanismos correspondientes para su acceso.
- En un ambiente multiusuario no se deberán compartir datos personales, excepto que se establezca por escrito la protección de datos personales con el fin de conceder privilegios en función de los roles y responsabilidades para el cumplimiento de sus deberes, sin que se exponga al acceso, eliminación, copia o alteración no autorizados de la información.
- Ningún usuario, está autorizado a llevar consigo o sacar del Consejo cintas, discos ópticos, discos compactos, memorias o cualquier otro medio electrónico con aplicaciones o información propiedad del Consejo.
- Ningún usuario está autorizado a instalar, desinstalar o borrar parcialmente datos, información, bases de datos, paquetería o aplicaciones en los bienes informáticos y de telecomunicaciones propiedad del Consejo, ya sea equipo bajo su resguardo o de algún otro usuario.

Medidas de apremio y sanciones

- Las personas servidoras públicas que no cumplan lo establecido en las políticas o medidas de seguridad establecidas, podrán ser merecedores a las Sanciones Administrativas referidas en el artículo 75 de la *Ley General de Responsabilidades Administrativas*,

atendiendo a los roles y responsabilidades, así como la cadena de rendición de cuentas establecidos en el Inventario Institucional de Datos Personales.

- Son aplicables las sanciones y los procedimientos referidos en el Título Décimo Primero Medidas de Apremio y Responsabilidades de la LGPDPPSO.
- Y las que correspondan a la materia artículo 163 de la LGPDPPSO y el 49 fracción V de la LGRA.

VII. Glosario.

Para efectos de la aplicación de las políticas se entenderá por:

Aviso de privacidad: Documento de forma física, electrónica o en cualquier formato, que es generado por el responsable y puesto a disposición de los titulares de los datos personales, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos.

Bases de datos: Conjunto ordenado de datos personales bajo criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

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 éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda;

Confidencialidad: Garantizar que la información es accesible sólo para aquellos autorizados a tener acceso.

Comité de Transparencia: Instancia a la que hace referencia el artículo 43 de la Ley General de Transparencia y Acceso a la Información Pública.

CONEVAL: Consejo Nacional de Evaluación de la Política de Desarrollo Social.

Consentimiento: Manifestación de la voluntad libre, específica e informada del titular de los datos mediante la cual se efectúa el tratamiento de los mismos.

Contraseña: Se refiere a aquella configuración lógica consistente en un conjunto de caracteres que se utiliza como herramienta para dar cierto grado de seguridad y de restricción de configuración, de administración o de servicios, con el propósito de evitar intrusiones o mal uso de los recursos que brinda el Consejo.

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

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. De manera enunciativa más no limitativa, se consideran sensibles 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 y preferencia sexual.

La LGPDPSO / señala 3 supuestos:

- Se refieran a su esfera más íntima de su titular.
- Aquellos cuya utilización indebida pueda dar origen a discriminación.

- Aquellos cuya utilización indebida conlleve un riesgo grave para su titular.

Adicionalmente a los descriptos en la definición pueden ser los siguientes:

- Datos que permiten conocer la ubicación física de una persona. (dirección física e información relativa al tránsito de las personas dentro y fuera del país)
- Datos que permitan inferir el patrimonio de una persona (los saldos bancarios, estados y/o número de cuenta, cuentas de inversión, bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos, egresos, buró de crédito, seguros, afores y fianzas. Incluye el número de tarjeta bancaria de crédito y/o débito)
- Datos de autenticación (usuarios, contraseñas, información biométrica (huellas dactilares, iris, voz, entre otros), firma autógrafa y electrónica y cualquier otro que permita autenticar a una persona.)
- Datos jurídicos (antecedentes penales, amparos, demandas, contratos, litigios y cualquier otro tipo de información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa). Entre otros, afiliación sindical.

Derechos ARCO: Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.

Derechos Morales: Está relacionada, de manera enunciativa más no limitativa, con sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, configuración y aspecto físicos, consideración que de sí mismo tienen los demás, o cuando se menoscabe ilegítimamente la libertad o la integridad física o psíquica de éste.

Derechos Patrimoniales: Está relacionada, de manera enunciativa más no limitativa, con sus bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados o las cantidades o porcentajes relacionados con la situación económica del titular.

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

Encargado: Persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable.

INAI: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, el cual es el organismo garante de la Federación en materia de protección de datos personales en posesión de los sujetos obligados.

Inventario: Inventario de Datos Personales y de sistemas del CONEVAL

LGPDPSSO: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Lineamientos Generales: Lineamientos Generales de Protección de Datos Personales para el Sector Público.

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

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, sus instalaciones físicas, áreas críticas, recursos e información;
- b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
- c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y
- d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

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 o a la información, 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.

Responsable: Los sujetos obligados a que se refiere el artículo 1 de la presente LGPDPPSO que deciden sobre el tratamiento de datos personales.

Revisión: Actividad estructurada, objetiva y documentada, llevada a cabo con la finalidad de constatar el cumplimiento continuo de los contenidos establecidos en este Programa.

Riesgo: Evento adverso e incierto (externo o interno) que derivado de la combinación de su probabilidad de ocurrencia y el posible impacto pudiera vulnerar los datos personales en posesión del CONEVAL.

Servidor Público: Las personas que desempeñan un empleo, cargo o comisión en los entes públicos, en el ámbito federal y local, conforme a lo dispuesto en el artículo 108 de la Constitución Política de los Estados Unidos Mexicanos.

Sistema de Gestión: Conjunto de reglas y principios relacionados entre sí de forma ordenada, para contribuir a la gestión de procesos específicos de una organización, en este caso en particular relativo a la protección de los datos personales en posesión del Coneval.

Titular: Persona física a quien corresponden los datos personales.

Transferencias: Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado.

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

El tratamiento consiste en la obtención de los datos, por ello se pone a disposición previamente a su obtención el aviso de privacidad en donde se canaliza al mecanismo de autenticación.

Unidad administrativa: Área a la que se le confiere atribuciones específicas en el estatuto orgánico, propietaria de procesos en los cuales se da tratamiento de datos personales.

Unidad de Transparencia: Instancia a la que hace referencia el artículo 45 de la Ley General de Transparencia y Acceso a la Información Pública.

Vulneraciones de seguridad: Afectaciones por el uso de datos personales, que de forma significativa afecten los derechos patrimoniales o morales del titular (pérdida o destrucción no autorizada; robo o extravío o copia no autorizada; el uso, acceso o tratamiento no autorizado; daño, alteración o modificación no autorizada; entre otras).

VIII. Anexos

Carta de confidencialidad.

Formato Inventario Institucional Datos Personales.

Formato Inventario sistemas.

Formato análisis de brecha.

Bitácora seguimiento y actualización avisos de privacidad.

Formato análisis de riesgos.

Documento Roles

Protocolo Derechos ARCO

Transitorios

Primero. - Las presentes políticas internas entrarán en vigor el día siguiente de su aprobación.

Segundo. - Las presentes políticas internas deberán ser publicadas en la página web institucional del CONEVAL.

Las presentes *Políticas internas para la gestión y tratamiento de los datos personales en posesión del CONEVAL*, fueron aprobadas por unanimidad de votos por los integrantes del Comité de Transparencia del Consejo Nacional de Evaluación de la Política de Desarrollo Social, mediante ACUERDO No. CT-O-03/11-2019/03, tomado en la Tercera Sesión Ordinaria del Comité de Transparencia, celebrada en la Ciudad de México, el 11 de diciembre de 2019.

Firman y rubrican el presente documento para constancia.

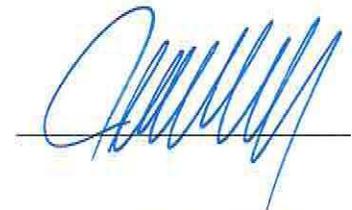
Nombre y cargo

Lcdo. Daniel Gutiérrez Cruz
Director General Adjunto de Administración
y Titular de la Unidad de Transparencia

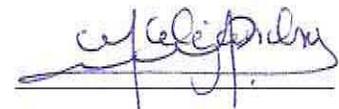
Firma



Lcdo. Fernando Moscoso Pohlenz
Titular del Órgano Interno de Control en el CONEVAL



Lcda. Martha Alejandra Mares Poletti
Directora Ejecutiva de Mejora de la Gestión y Archivo
y Responsable del Área Coordinadora de Archivos



Protocolo para ejercer los Derechos ARCO en el Consejo Nacional de Evaluación de la Política de Desarrollo Social (CONEVAL)

I. Introducción

En cumplimiento a lo dispuesto en los artículos 6°, base A, fracción II, 16, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos; 33, fracción I, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPSSO); y 56, fracción VI, de los Lineamientos Generales de Protección de Datos Personales para el Sector Público; el CONEVAL elaboró el presente Protocolo para ejercer los Derechos ARCO.

II. Glosario

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

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. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

Derechos ARCO: Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.

Estado de Interdicción: Es una condición jurídica que afecta a aquellos individuos que no tienen capacidad de tomar decisiones por sí mismos en razón de un trastorno mental, en consecuencia se encuentran limitados en cuanto a su conciencia y por tal motivo es necesario nombrar un representante legal que debe atender la vida jurídica del individuo.

III. Políticas generales

1. Para ejercer alguno de los derechos de acceso, rectificación, cancelación u oposición al tratamiento de sus datos personales, conocidos como derechos ARCO, la persona solicitante debe tomar en cuenta que el derecho a la protección de datos personales es un derecho personalísimo, por lo que sólo el titular de los datos personales o, en su caso, su representante legal podrán solicitarlo.
2. Cuando la información proporcionada por el titular en su solicitud sea insuficiente para atenderla, el CONEVAL deberá prevenir al titular, por una sola vez y dentro de los cinco días contados a partir del día siguiente al que recibió la solicitud, para que aporte los elementos o documentos necesarios para dar trámite a la misma. Se tendrán 10 días hábiles, para proporcionar la información requerida, pues de lo contrario se tendrá como no presentada dicha solicitud.

3. Una vez presentada una solicitud, se deberá entregar a la persona solicitante, un ACUSE en el que conste la fecha de recepción de la misma.
4. Entre las identificaciones oficiales válidas se encuentran: credencial para votar, pasaporte, cartilla militar, cédula profesional, licencia para conducir y documento migratorio.
5. La personalidad de su representante legal, en su caso, se podrá acreditar, cuando se trate de una persona física, se podrá elegir cualquiera de las siguientes tres opciones:
 - a) La presentación de una carta poder simple suscrita ante dos testigos, anexando copia simple de sus identificaciones oficiales.
 - b) Mediante instrumento público (documento suscrito por un Notario Público).
 - c) Acudiendo usted y su representante a declarar en comparecencia ante el responsable.
6. Es importante tener en cuenta que la identidad del titular y su representante legal, así como la personalidad de este último, deberán quedar debidamente acreditadas previo al ejercicio del derecho de que se trate, en caso de que resulte procedente, mediante la presentación de los documentos originales antes señalados o copia certificada de los mismos, para su cotejo.
7. Para el caso de solicitudes relacionadas con datos personales de menores de edad, personas en estado de interdicción o incapacidad declarada por ley, el ejercicio de derechos ARCO de este grupo de titulares, además de la presentación de la solicitud con la información descrita en el numeral 1, se deberán presentar, según sea el caso, los siguientes documentos:

<p>Cuando los padres ejercen la patria potestad:</p>	<ul style="list-style-type: none"> • Documento que acredite la identidad de menor. • Acta de nacimiento del menor. • Identificación oficial del padre o de la madre, que pretenda ejercer el derecho. • Carta en la que se manifieste, bajo protesta de decir verdad, que el padre o la madre es quien ejerce la patria potestad del menor, y que no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de la patria potestad. <p>Si una persona distinta a los padres es quien ejerce la patria potestad, y es quien presenta la solicitud:</p> <ol style="list-style-type: none"> a) Documento que acredite la identidad de menor. b) Acta de nacimiento del menor. c) Documento legal que acredite la posesión de la patria potestad. d) Identificación oficial de quien presenta la solicitud y posee la patria potestad. e) Carta en la que se manifieste, bajo protesta de decir verdad, que ejerce la patria potestad del menor, y que no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de la patria potestad.
<p>Cuando un tutor es quien ejerce la patria potestad:</p>	<ul style="list-style-type: none"> • Documento que acredite la identidad de menor. • Acta de nacimiento del menor. • Documento legal que acredite la tutela. • Identificación oficial del tutor.

	<ul style="list-style-type: none"> • Carta en la que se manifieste, bajo protesta de decir verdad, que ejerce la tutela del menor, y que no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de la tutela.
Personas en estado de interdicción o incapacidad legal	<p>Documento que acredite la identidad del titular de los datos personales.</p> <ul style="list-style-type: none"> • Instrumento legal de designación del tutor. • Identificación oficial del tutor. • Carta en la que se manifieste, bajo protesta de decir verdad, que ejerce la tutela, y que no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de la misma.

Procedimientos

Para la presentación y atención de una solicitud de ejercicio de derechos ARCO es necesario realizar lo siguiente:

A. Presentación de una solicitud de ejercicio de derechos ARCO.

1. Presentar la solicitud ante la Unidad de Transparencia del CONEVAL, a través de los medios y mecanismos señalados en el aviso de privacidad, con la siguiente información:

- a) Nombre del titular de los datos personales.
- b) Documentos que acrediten la identidad del titular.
- c) En su caso, nombre del representante legal del titular y documentos para acreditar su identidad y personalidad.
- d) Especificar el medio para recibir notificaciones.
- e) Descripción clara y precisa de los datos personales que se quieran rectificar, cancelar u oponerse a su tratamiento.
- f) Descripción del derecho que se quiere ejercer o de lo que solicita el titular.
- g) En su caso, documentos o información que faciliten la localización de los datos personales, entre ella, la unidad administrativa responsable del tratamiento.
- h) Información específica. Además de la información general antes señalada, dependiendo del derecho que desee ejercer, deberá precisarlo:
 - Derecho de ACCESO: la modalidad en la que prefiere que se reproduzcan los datos personales solicitados.
 - Derecho de RECTIFICACIÓN: las modificaciones que solicita que se realicen a los datos personales, así como aportar los documentos que sustenten la solicitud.
 - Derecho de CANCELACIÓN: las causas que motivan la petición de que se eliminen los datos de los archivos, registros o bases de datos del responsable del tratamiento.
 - Derecho de OPOSICIÓN: las causas o la situación que lo llevan a solicitar que finalice el tratamiento de sus datos personales, así como el daño o perjuicio que le causaría que

dicho tratamiento continúe; o bien, deberá indicar las finalidades específicas respecto de las cuales desea ejercer este derecho.

2. Acreditar la identidad del titular y, en su caso, la de su representante legal, así como la personalidad de este último.

3. La solicitud se deberá acompañar de copia simple de una identificación oficial del titular de los datos personales, así como de su representante legal, en caso de que éste sea quien presente la solicitud.

Plazos y procedimiento para la atención de las solicitudes de ejercicio de derechos ARCO

Toda vez que se presente una solicitud y se confirme que ésta cumplió con los requisitos antes descritos, el CONEVAL a través de la Unidad de Transparencia deberá realizar lo siguiente:

- En un plazo de 20 días hábiles, contados a partir del día siguiente a la recepción de la solicitud, deberá informar a la persona solicitante si procede o no el ejercicio del derecho solicitado.
- En caso de que haya procedido el ejercicio del derecho, en un plazo de 15 días hábiles, contados a partir del día siguiente en el que le haya notificado la respuesta anterior, el CONEVAL deberá llevar a cabo las acciones necesarias para hacerlo efectivo.
- Los plazos antes señalados se pueden ampliar por un periodo igual, cuando esté justificado y se le informe de ello.
- El ejercicio de los derechos ARCO será sencillo y gratuito, sólo podrán realizarse cobros para recuperar los costos de reproducción, certificación de documentos o envío de información.
- Si la misma persona reitera su solicitud de acceso en un periodo menor a 12 meses, los costos no serán mayores a tres veces el valor diario de la Unidad de Medida y Actualización (UMA), a menos que existan modificaciones sustanciales al aviso de privacidad que motiven nuevas consultas.
- Cuando las disposiciones aplicables a determinadas bases de datos o tratamientos establezcan un procedimiento específico, se estará a lo dispuesto en aquéllas que ofrezcan mayores garantías al titular, y no contravengan las disposiciones previstas en la Ley.

Dentro de un plazo que no podrá exceder de quince días contados a partir del siguiente a la fecha de la notificación de la respuesta, el Titular de los datos personales podrá presentar un recurso de revisión ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), por la respuesta recibida o falta de ésta.

El CONEVAL garantizará la privacidad de los particulares y deberá velar porque terceras personas no incurran en conductas que puedan afectarla arbitrariamente. Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, se establecen y mantienen 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.

En caso de dudas comunicarse a la Unidad de Transparencia: Email: unidadtransparencia@coneval.org.mx, Tel: 55-5481-7282.

DISPOSICIONES TRANSITORIAS

PRIMERA. El presente Protocolo entrará en vigor el día hábil siguiente a la fecha de aprobación por parte del Comité de Transparencia del CONEVAL.

SEGUNDA. Este Protocolo se publicará en la página web del CONEVAL.

El presente Protocolo se expide en la Ciudad de México, el 11 de diciembre de 2019.