



# **POLÍTICAS INTERNAS PARA LA GESTIÓN Y EL TRATAMIENTO DE LOS DATOS PERSONALES EN POSESIÓN DE LA COMISIÓN NACIONAL DE SEGUROS Y FIANZAS**



**HACIENDA**  
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO



COMISIÓN NACIONAL  
DE SEGUROS Y FIANZAS



**Contenido**

PRESENTACIÓN..... 2

FUNDAMENTO LEGAL ..... 2

OBJETIVO..... 2

ÁMBITO DE APLICACIÓN ..... 2

POLÍTICAS INTERNAS PARA LA GESTIÓN Y EL TRATAMIENTO DE LOS DATOS PERSONALES EN POSESIÓN DE LA COMISIÓN NACIONAL DE SEGUROS Y FIANZAS ..... 3

CAPÍTULO I..... 3

Disposiciones generales ..... 3

CAPÍTULO II ..... 5

De los principios ..... 5

CAPÍTULO III..... 8

De los deberes ..... 8

CAPÍTULO IV..... 9

De las obligaciones..... 9

Identificación del ciclo de vida de los datos personales ..... 10

CAPÍTULO V ..... 10

De la imposición de sanciones por incumplimiento a la protección de datos personales..... 10

DISPOSICIONES TRANSITORIAS ..... 12





## PRESENTACIÓN

La Comisión Nacional de Seguros y Fianzas es un Órgano Desconcentrado de la Secretaría de Hacienda y Crédito Público, encargada de supervisar que la operación de los sectores asegurador y afianzador se apegue al marco normativo, preservando la solvencia y estabilidad financiera de las instituciones de seguros y fianzas, para garantizar los intereses del público usuario, así como promover el sano desarrollo de estos sectores con el propósito de extender la cobertura de sus servicios a la mayor parte posible de la población.

En este sentido, conforme los artículos 1 y 3 fracción XXVIII de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, este Órgano Desconcentrado, en su carácter de sujeto obligado es responsable de proporcionar un correcto tratamiento de los datos personales en su posesión de acuerdo con los principios, deberes y obligaciones que establece la normatividad en la materia, a fin de establecer y mantener las medidas de seguridad para la protección de estos, al crear políticas internas para la gestión y el 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.

Para dar cumplimiento a lo anterior, el artículo 47 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, establece la obligación de instrumentar políticas que definan los elementos, así como las actividades que las instituciones deben llevar a cabo para dirigir, operar y controlar todos los procesos que impliquen el tratamiento de datos personales, con el propósito de protegerlos de manera sistemática y continua, conforme el artículo 56 de los referidos preceptos normativos.

## FUNDAMENTO LEGAL

El presente documento normativo se emite de conformidad con los artículos 30 fracciones I y II, 33 fracción I, 83 y 84 fracción I de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como el artículo 47 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

## OBJETIVO

Instrumentar las directrices normativas que rijan las actividades internas de la Comisión Nacional de Seguros y Fianzas para cumplir con los principios, deberes y obligaciones previstos por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en el tratamiento de datos personales a fin de garantizar el derecho humano a la protección de datos personales que establece el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos.

## ÁMBITO DE APLICACIÓN

Son de observancia general y aplicación obligatoria para todas las personas servidoras públicas de la Comisión Nacional de Seguros y Fianzas que conforme a sus atribuciones realicen tratamiento de datos personales, así como para terceros, que como encargados o por la prestación de algún servicio lleven a cabo el tratamiento de datos personales en posesión de este sujeto obligado o conozcan por alguna circunstancia de éstos.



## POLÍTICAS INTERNAS PARA LA GESTIÓN Y EL TRATAMIENTO DE LOS DATOS PERSONALES EN POSESIÓN DE LA COMISIÓN NACIONAL DE SEGUROS Y FIANZAS

### CAPÍTULO I Disposiciones generales

**Primero.** Las presentes políticas tienen por objeto establecer las acciones generales, así como los mecanismos para dar cumplimiento a los principios, deberes, derechos y obligaciones previstas por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

Para efectos de las presentes políticas se entenderá por:

- I. **Áreas responsables:** Unidades administrativas de la Comisión que realicen tratamiento de datos personales, las cuales serán responsables de dar cumplimiento a los principios, deberes y obligaciones establecidas en la Ley General.
- II. **Aviso de privacidad:** Documento que se disposición de las personas titulares de los datos personales de forma física, electrónica o en cualquier formato generado por las áreas responsables, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de estos.
- III. **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 eliminación en la base de datos o formatos de almacenamiento que correspondan.
- IV. **Comité de Transparencia:** Órgano colegiado que para efectos de las presentes políticas cuenta con las atribuciones señaladas por el artículo 84 de la Ley General, el cual dentro de la Comisión es la autoridad máxima en materia de protección de datos personales.
- V. **Comisión:** La Comisión Nacional de Seguros y Fianzas.
- VI. **Consentimiento:** Manifestación de la voluntad libre, específica e informada de la persona titular de los datos personales mediante la cual se efectúa el tratamiento de estos.
- VII. **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.
- VIII. **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.
- IX. **Derechos ARCO:** Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales, entendidos de la siguiente manera:
  - a. **Acceso:** Las personas titulares tienen el derecho de acceder a sus datos personales que obren en posesión de las áreas responsables de la Comisión.
  - b. **Rectificación:** El derecho de las personas titulares a la corrección de sus datos personales, cuando estos resulten ser inexactos, incompletos o no se encuentren actualizados.
  - c. **Cancelación:** Las personas titulares tienen el derecho a solicitar la cancelación de sus datos personales de los archivos, registros, expedientes y sistemas de las áreas responsables de la Comisión, a fin de que los mismos ya no estén en su posesión y dejen de ser tratados.
  - d. **Oposición:** El derecho de las personas titulares al cese del tratamiento de sus datos personales cuando el tratamiento le cause un daño o perjuicio y cuando 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 de su titular o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.

- X. **Documento de seguridad:** Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por la Comisión para garantizar la confidencialidad, integridad y disponibilidad de los datos personales en su posesión.
- XI. **Encargado:** La persona física o jurídica, pública o privada, ajena a la Comisión, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta de este sujeto obligado.
- XII. **Evaluación de impacto en la protección de datos personales:** Documento mediante el cual las áreas 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, valorarán los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de las personas titulares, así como los deberes de los responsables y encargados, previstos en la normativa aplicable.
- XIII. **Instituto:** El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.
- XIV. **Ley General:** La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- XV. **Lineamientos Generales:** Los Lineamientos Generales de Protección de Datos Personales para el Sector Público.
- XVI. **Medidas de seguridad:** Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.
- XVII. **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.
- XVIII. **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 a las instalaciones físicas de la Comisión donde se realice el tratamiento de datos personales, así como las áreas críticas, recursos físicos y tecnológicos e información.
  - b. Prevenir el daño o interferencia a las instalaciones físicas, recursos e información.
  - c. Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la Comisión.
  - d. Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.
- XIX. **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. Asegurar que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados.
  - b. Identificar y gestionar las funciones que las personas que dan tratamiento de datos personales realicen en cumplimiento de sus actividades institucionales.
  - c. Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware de los activos tecnológicos.
  - d. Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.



- XX.** **Remisión:** Toda comunicación de datos personales realizada exclusivamente entre la Comisión y el encargado, dentro o fuera del territorio mexicano.
- XXI.** **Sujeto obligado:** Cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, del ámbito federal. Titular: La persona física a quien corresponden los datos personales.
- XXII.** **Titular:** La persona física a quien corresponden los datos personales.
- XXIII.** **Transferencia:** Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, de la Comisión o del encargado.
- XXIV.** **Tratamiento de datos personales:** 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.
- XXV.** **Unidad de Transparencia:** Área administrativa de la Comisión encargada de coordinar el cumplimiento de las disposiciones normativas en materia de protección de datos personales, así como de instrumentar las resoluciones que emita el Comité de Transparencia. Para efectos derivados de las presentes políticas, se integrará y funcionará conforme lo previsto por el artículo 85 de la Ley General.

**Segundo.** Las políticas serán aplicables a cualquier tratamiento de datos personales que obre en soportes físicos, electrónicos o mixtos, ya sea que su uso se realice mediante procedimientos manuales o automatizados, sin excepción de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

**Tercero.** El Comité de Transparencia a través de la Unidad de Transparencia garantizará la privacidad de los individuos, la protección de los datos personales en posesión de la Comisión y deberá velar porque las áreas responsables, así como terceras personas no incurran en conductas que puedan afectar arbitrariamente a los titulares de los datos personales. Para lo anterior, la Unidad de Transparencia podrá emitir guías, infografías y material audiovisual que facilite a las áreas responsables el cumplimiento de los principios, deberes y obligaciones en materia de protección de datos personales.

## CAPÍTULO II De los principios

**Cuarto.** En todo tratamiento de datos personales deberán observarse los siguientes principios rectores de la protección de datos personales, mismos que se encuentran señalados en el artículo 7 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público:

- I.** Licitud.
- II.** Finalidad.
- III.** Lealtad.
- IV.** Consentimiento.
- V.** Calidad.
- VI.** Proporcionalidad.
- VII.** Información.
- VIII.** Responsabilidad.

**Quinto.** Todo tratamiento de datos personales deberá realizarse conforme a las atribuciones o facultades que la normatividad aplicable les confiera a las áreas responsables, quienes solo podrán tratar los datos personales para aquello a lo que estén legalmente facultados.

Para cumplir con el principio de licitud, deberá incluirse en cada aviso de privacidad integral el fundamento legal que sustente el tratamiento de datos personales.





**Sexto.** Los datos personales deben ser tratados exclusivamente para cumplir con las fines para los cuales fueron recabados, debiendo ajustarse las finalidades a lo siguiente:

- I. **Concretas.** Deberán atender a la consecución de fines específicos o determinados, sin que se admitan errores, distintas interpretaciones o provoquen incertidumbre, dudas o confusión en las personas titulares.
- II. **Explícitas.** Al darse a conocer de manera clara en el aviso de privacidad.
- III. **Lícitas.** Por justificar que el tratamiento de los datos personales sea acorde con las atribuciones o facultades del área responsable, conforme a lo previsto en la legislación mexicana y el derecho internacional que le resulte aplicable.
- IV. **Legítimas.** Por contar con el consentimiento de la persona titular de los datos personales, cuando este sea necesario.

Corresponderá a las áreas responsables identificar las finalidades de cada tratamiento de datos personales que realicen conforme sus atribuciones institucionales, así como verificar si al momento de recabar los datos personales deba obtenerse el consentimiento de las personas titulares para su tratamiento.

**Séptimo.** Las áreas responsables establecerán los procedimientos adecuados para que los datos personales no se obtengan con dolo, mala fe o negligencia.

De igual manera deberán procurar que el tratamiento de datos personales que se efectúe no dé lugar a discriminación ni trato injusto en contra de cualquier persona titular.

Para cumplir con el principio de lealtad, los avisos de privacidad deberán reflejar la realidad del tratamiento que se lleve a cabo.

**Octavo.** Al recabar datos personales, deberá proporcionarse a los titulares de datos personales el aviso de privacidad simplificado o integral.

Cuando los datos personales no se recaben directamente de su titular, éste tendrá un plazo de cinco días, contados a partir del día siguiente de recibir el aviso de privacidad, para que, en su caso, manifieste su negativa al tratamiento de sus datos personales a través de los medios que correspondan. Agotado dicho plazo, se entenderá que ha otorgado su consentimiento tácito para el tratamiento de sus datos personales.

No será necesario obtener el consentimiento expreso de las personas titulares cuando se actualice alguna de las siguientes causales:

- I. Cuando una ley así lo disponga, siempre y cuando dicho ordenamiento no contravenga las bases, principios y disposiciones establecidas en la Ley General.
- II. Cuando el tratamiento de los datos personales implique transferencias de estos entre responsables por razones compatibles con las finalidades que dieron origen a su obtención.
- III. Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente.
- IV. Para el reconocimiento o defensa de derechos de la persona titular ante autoridad competente.
- V. Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre la persona titular y la Comisión.
- VI. Cuando exista una situación de emergencia que potencialmente pueda dañar a una persona en su individualidad 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.



En caso de que no se actualice alguna de las causales anteriores, las áreas responsables deberán obtener el consentimiento expreso y por escrito de los titulares para el tratamiento de sus datos personales mediante el aviso de privacidad, a través de su firma autógrafa, firma electrónica o cualquier mecanismo de autenticación que para el efecto se establezca.

**Noveno.** Las áreas responsables deberán 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, asegurando que cumplan con lo siguiente:

- I. **Exactos.** Que los datos personales en posesión de las áreas responsables no presenten errores que afecten su veracidad.
- II. **Completos.** Que su integridad permita el cumplimiento de las finalidades que originaron su tratamiento.
- III. **Actualizados.** Que los datos personales responden fielmente a la situación actual de su titular.
- IV. **Correctos.** Que cumplan con todas las características anteriores.

Para atender el principio de calidad, las áreas responsables deberán implementar mecanismos que permitan corregir los datos personales en las distintas bases o sistemas electrónicos que estén a su cargo, cuando derivado de sus funciones adviertan la existencia de alguna inconsistencia generada durante su tratamiento, lo cual deberá documentarse.

Se presume que se cumple con la calidad en los datos personales cuando éstos son proporcionados directamente por la persona titular y hasta que ésta no manifieste y acredite lo contrario. Por otra parte, cuando los datos personales sean obtenidos indirectamente de la persona titular, se deberán adoptar medidas de cualquier naturaleza dirigidas a garantizar que éstos cumplan con el principio de calidad.

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, deberán ser suprimidos o eliminados, previo bloqueo en su caso, una vez que concluya su plazo de conservación de conformidad con el ciclo de vida establecido por las áreas responsables.

**Décimo.** Para cumplir con el principio de proporcionalidad, las áreas responsables serán las encargadas de identificar y recabar solo aquellos datos personales que resulten adecuados, relevantes y necesarios para cada una de las finalidades de los tratamientos que realicen.

Lo anterior se materializa cuando los datos personales son apropiados, indispensables y no excesivos para el cumplimiento de los fines que motivaron su obtención.

Cuando una norma establezca con precisión los datos personales que deberán someterse a tratamiento, no deberán recabarse más datos de los requeridos.

**Décimo primero.** Las áreas responsables deberán informar a las personas titulares a través del aviso de privacidad, la existencia, características y finalidades del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.

Por lo anterior, es obligación de las áreas responsables la elaboración, difusión y actualización del aviso de privacidad que corresponda a cada tratamiento de datos personales. Para su presentación se deberá:

- I. Elaborar en versión simplificada e integral.
- II. Redactar de manera clara y sencilla, con una estructura y diseño que facilite su comprensión.
- III. Poner a disposición de las personas titulares en los medios donde se obtengan sus datos personales.



- IV. Habilitar los mecanismos necesarios para solicitar el consentimiento expreso de las personas titulares de los datos personales cuando sea necesario.
- V. Comunicar el aviso de privacidad a encargados y terceros a quienes se remitan o transfieran datos personales.
- VI. Informar al Comité de Transparencia de la Comisión a través de la Unidad de Transparencia cuando se realicen actualizaciones en los avisos de privacidad.

Para dar cumplimiento al principio de información, las áreas responsables deberán contar con las evidencias que acrediten, según sea el caso, la ejecución de las acciones mencionadas en las fracciones anteriores.

**Décimo segundo.** Las áreas responsables bajo la coordinación del Comité de Transparencia por conducto de la Unidad de Transparencia deberán adoptar las presentes políticas e implementar los mecanismos conducentes para asegurar el cumplimiento de los principios, deberes y obligaciones establecidos en la Ley General, los Lineamientos Generales, así como la demás normatividad en materia de protección de datos personales.

Lo anterior, también resultará aplicable cuando los datos personales sean tratados por parte de un encargado y al momento de realizar transferencias, nacionales o internacionales, de datos personales.

### **CAPÍTULO III** **De los deberes**

**Décimo tercero.** Es de observancia obligatoria en la Comisión, el cumplimiento de los siguientes deberes:

- I. **De seguridad.** Implica la implementación, mantenimiento y mejora de diversas medidas de carácter administrativas, físicas y técnicas para la protección de los datos personales contra daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado.
- II. **De confidencialidad.** Implica la implementación de controles que permitan a todas aquellas personas que intervengan en cualquier fase del tratamiento de datos personales, guardar confidencialidad respecto de estos, a efecto de evitar ocasionar cualquier daño a sus titulares, obligación que subsistirá aún después de finalizar las actividades derivadas de sus funciones.

**Décimo cuarto.** Para cumplir con el deber de seguridad, las áreas responsables deberán:

- I. Capacitar al personal que intervenga en el tratamiento de datos personales, a fin de sensibilizarles acerca de los riesgos inherentes, las posibles consecuencias para las personas titulares por alguna vulneración, la sensibilidad de los datos personales, el desarrollo tecnológico y sus obligaciones normativas.
- II. Determinar el ciclo de vida de los datos personales bajo tratamiento.
- III. Establecer y mantener medidas de seguridad administrativas, físicas y técnicas, considerando los riesgos y amenazas asociados al tratamiento de datos personales.
- IV. Coadyuvar en la actualización del documento de seguridad de la Comisión.
- V. Llevar a cabo las medidas preventivas y correctivas para mitigar las brechas de seguridad identificadas en el documento de seguridad.
- VI. Informar a la Unidad de Transparencia de cualquier modificación o cambios que se susciten en la información que reportan en el documento de seguridad.
- VII. Analizar la procedencia de obtener el consentimiento de las personas titulares, en cualquier transmisión de datos personales que se realice, lo cual se deberá notificar a la Unidad de Transparencia.
- VIII. Al contratar o adherirse a servicios, aplicaciones e infraestructura de cómputo en la nube y otras materias que impliquen el tratamiento de datos personales, el proveedor externo



deberá garantizar el cumplimiento de las obligaciones establecidas en los artículos 59, 63 y 64 de la Ley General. Corresponderá a la Dirección General de Sistemas cerciorarse de dicha circunstancia.

- IX.** En caso de suscitarse alguna vulneración a los datos personales sujetos a tratamiento, se deberá informar a la Unidad de Transparencia en un plazo no mayor a 24 horas a partir del momento en que se confirme la ocurrencia del incidente, con el propósito de activar el protocolo de acción conducente.

**Décimo quinto.** Para cumplir con el deber de confidencialidad, las áreas responsables deberán:

- I.** Capacitar al personal que interviene en el tratamiento de datos personales en temas orientados a sensibilizarles acerca la importancia de la confidencialidad y sus alcances.
- II.** Proporcionar la declaratoria de confidencialidad a todo el personal que intervenga en el tratamiento de datos personales a efecto de que conozcan sus responsabilidades y suscriban su compromiso de confidencialidad.
- III.** Guardar confidencialidad en cualquier fase del tratamiento de datos personales, incluso después de finalizar su relación con la Comisión.
- IV.** Incluir en los contratos u otros instrumentos jurídicos que celebren con terceros, cláusulas de confidencialidad.
- V.** Verificar que terceros encargados de información que contenga datos personales guarden confidencialidad de estos, aun después de concluida su relación con la Comisión.
- VI.** Comunicar a terceros receptores de datos personales, el aviso de privacidad integral correspondiente y documentar dicha comunicación.

## **CAPÍTULO IV** **De las obligaciones**

**Décimo sexto.** Es de observancia obligatoria entre el personal de la Comisión coadyuvar en el cumplimiento de la Ley General, así como los Lineamientos Generales y los demás instrumentos normativos en materia de protección de datos personales que emita el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

**Décimo séptimo.** Para el cumplimiento del numeral anterior, todas las personas que intervengan en cualquier tipo de tratamiento de datos personales, así como las áreas responsables deberán realizar lo siguiente:

- I.** Informar a la Unidad de Transparencia, de cualquier actividad que conlleve el tratamiento de datos personales que no se encuentre enlistada en el documento de seguridad de la Comisión.
- II.** Atender las solicitudes de derechos ARCO conforme procedimiento Interno difundido por la Unidad de Transparencia.
- III.** Revisar que las actividades de tratamiento de datos personales que se realicen cuenten con sus avisos de privacidad y estos se difundan en los medios desde los cuales se recaban los datos sujetos a tratamiento.
- IV.** Dar vista al Comité de Transparencia, a través de la Unidad de Transparencia, de cualquier vulneración o tratamiento indebido de datos personales de los que se tenga conocimiento.
- V.** Asegurar que el acceso a datos personales en posesión de la Comisión sea únicamente por el personal autorizado, conforme los fines, facultades y atribuciones descritas en el documento de seguridad. Por tal virtud, queda estrictamente prohibido proporcionar datos personales a quienes no se encuentren autorizados para su tratamiento.
- VI.** Cuando se pretenda poner en operación o modificar sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, se deberá realizar una evaluación de impacto en la protección de datos personales conforme la normatividad en la materia y presentarla ante la Unidad de Transparencia para que esta analice el protocolo a seguir.



- VII. Solicitar el asesoramiento del personal de la Unidad de Transparencia cuando estimen necesaria su intervención con el objeto dar cumplimiento a los principios, deberes y obligaciones en materia de protección de datos personales.

### Identificación del ciclo de vida de los datos personales

**Décimo octavo.** El ciclo de vida de los datos personales sujetos a tratamiento será determinado por las áreas responsables.

Para realizar lo anterior, será necesario que las áreas responsables identifiquen cada una de las etapas por las que pasan los datos personales desde su obtención hasta su eliminación, lo cual deberán integrar en el documento de seguridad de la Comisión.

**Décimo noveno.** En la definición del ciclo de vida de los datos personales, deberán enlistarse y clasificarse las fases por las que pasan los datos personales de acuerdo con las siguientes categorías:

- I. **Obtención.** Enunciar las circunstancias que dan origen a la obtención de los datos personales.
- II. **Almacenamiento.** Enunciar los medios en los que se almacenan los datos personales una vez que son obtenidos.
- III. **Uso.** Enunciar de manera consecutiva las fases por las que pasan los datos personales durante su procesamiento para cumplir con las finalidades por las que fueron obtenidos.
- IV. **Divulgación.** Enunciar si los datos personales son transferidos a terceros, remitidos a encargados y, de ser el caso, la denominación de estos terceros implicados.
- V. **Bloqueo.** Enunciar el mecanismo empleado para conservar los datos personales una vez cumplida la finalidad por la que fueron recabados.
- VI. **Eliminación.** Enunciar el proceso mediante el cual son destruidos, borrados o suprimidos los datos personales.

**Vigésimo.** Al determinar el ciclo de vida de los datos personales, las áreas responsables deberán establecer los plazos de conservación de los mismos, observando, a su vez, las temporalidades establecidas en su Catálogo de Disposición Documental.

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.

## CAPÍTULO V

### De la imposición de sanciones por incumplimiento a la protección de datos personales

**Vigésimo primero.** De conformidad con el artículo 105 de los Lineamientos Generales, cuando alguna área responsable se niegue a colaborar con la Unidad de Transparencia en la atención de las solicitudes para el ejercicio de los derechos ARCO, ésta deberá dar aviso al superior jerárquico del área responsable para que le ordene realizar sin demora las acciones conducentes.

Si persiste la negativa de colaboración, la Unidad de Transparencia lo hará del conocimiento del Comité de Transparencia para que, a su vez, dé vista al Órgano Interno de Control Específico y, de resultar procedente se dé inicio el procedimiento de responsabilidad administrativo respectivo.

**Vigésimo segundo.** Cuando el Comité de Transparencia tenga conocimiento del incumplimiento de alguna obligación prevista en la Ley General, las presentes políticas o demás normas exigibles en materia de protección de datos personales, por conducto de la Unidad de Transparencia,





realizará un exhorto al área responsable para que lleve a cabo las acciones pertinentes con objeto de modificar dicha situación, evitar incumplimientos o situaciones de riesgo que se puedan suscitar.

Además, el Comité de Transparencia tomará las medidas necesarias para que las personas servidoras públicas que están a cargo del tratamiento de datos personales conozcan las causas de sanción por incumplimiento de las obligaciones establecidas en la Ley General, así como los Lineamientos Generales.

**Vigésimo tercero.** El Instituto podrá imponer las siguientes medidas de apremio para asegurar el cumplimiento de sus determinaciones:

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

Las medidas de apremio de carácter económico no podrán ser cubiertas con recursos públicos. El incumplimiento a las obligaciones en materia de protección de datos personales será difundido en los portales de obligaciones de transparencia del Instituto y considerado en las evaluaciones que realice.

**Vigésimo cuarto.** De conformidad con el artículo 163, serán causas de incumplimiento de las obligaciones en materia de protección de datos personales, 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 la Ley General 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 custodia del área responsable correspondiente o a los cuales tenga 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 en la Ley General y las presentes políticas.
- V. No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos a que refiere el artículo 27 de la Ley General, 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 la normatividad aplicable.
- VII. Incumplir el deber de confidencialidad establecido en el artículo 42 de la Ley General y las presentes políticas.
- VIII. No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la Ley General.
- IX. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad según los artículos 31, 32 y 33 de la Ley General.
- X. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la Ley General y las presentes políticas.
- XI. Obstruir los actos de verificación del Instituto o del Comité de Transparencia por conducto de la Unidad de Transparencia.
- XII. No acatar las resoluciones emitidas por el Instituto.

Las causas de responsabilidad previstas en las fracciones I, II, IV, VI y X, así como la reincidencia en las conductas previstas en el resto de las fracciones de este artículo, serán consideradas como faltas graves para efectos de su sanción administrativa.



**Vigésimo quinto.** Para las conductas a que se refiere el artículo anterior el Instituto dará vista a la autoridad competente para que imponga o ejecute la sanción.

### DISPOSICIONES TRANSITORIAS

**PRIMERA.** Una vez aprobado el presente documento normativo, para su debida aplicación y vigencia, la Unidad de Transparencia se encargará de notificar las Políticas Internas para la Gestión y el Tratamiento de los Datos Personales en Posesión de la Comisión Nacional de Seguros y Fianzas a todas las personas servidoras públicas que laboran en este sujeto obligado.

**SEGUNDA.** A través de la Unidad de Transparencia, se publicarán los presentes Lineamientos en el portal institucional de esta Comisión.

Así lo resolvieron por unanimidad de votos las personas integrantes del Comité de Transparencia de la Comisión Nacional de Seguros y Fianzas, a los treinta días del mes de mayo de dos mil veinticuatro, en el Tema Primero, asentado en el acta de la Tercera Sesión Ordinaria, disponible para su consulta en la siguiente liga electrónica:

- [Acta de la Tercera Sesión Ordinaria \(UT\\_CNSF\)](#)