



**CENACE**<sup>®</sup>

CENTRO NACIONAL DE  
CONTROL DE ENERGÍA

# **PROGRAMA DE PROTECCIÓN DE DATOS PERSONALES.**

## Contenido

INTRODUCCIÓN. ....	3
MARCO JURÍDICO. ....	5
GLOSARIO. ....	6
OBJETIVO. ....	9
RESPONSABILIDADES DENTRO DEL PROGRAMA. ....	10
ALCANCE DEL PROGRAMA. ....	11
CUMPLIMIENTO DE OBLIGACIONES. ....	12
FUNCIONES DEL COMITÉ DE TRANSPARENCIA. ....	15
FUNCIONES DE LA UNIDAD DE TRANSPARENCIA. ....	16
CAPACITACIÓN. ....	17
REVISIONES Y AUDITORIAS. ....	18
LA DEFINICIÓN DE ACCIONES PARA LA MEJORA CONTINUA. ....	19
SANCIONES.....	20

## **INTRODUCCIÓN.**

El derecho a la protección de datos personales se introduce por primera vez en México a través de la ahora abrogada Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental de 2002, que establecía dentro de sus objetivos el de "Garantizar la protección de datos personales en posesión de sujetos obligados" (artículo 3, fracción III), así como un desarrollo incipiente de los principios, derechos y deberes que lo conforman.

En ese sentido, el derecho a la protección de datos personales sería inicialmente un límite o excepción del derecho de acceso a la información, cuyo campo de aplicación cobraría mayor fuerza, más como un criterio de clasificación de la información que como un derecho subjetivo propio a favor de la dignidad humana y la autodeterminación informativa.

Con la reforma constitucional de 2009 a los artículos 16 y 73, fracción XXIX-0 se produce un verdadero cambio de paradigma que dota al derecho a la protección de datos personales de un contenido propio e independiente del derecho de acceso a la información pública. Mediante esta reforma constitucional se extiende, en todo el territorio nacional, el ámbito de protección de las personas por lo que se refiere a sus datos personales mediante la incorporación de los particulares como responsables de su tratamiento. Para esos efectos, la reforma constitucional le confiere al Congreso de la Unión la facultad para legislar de manera exclusiva en la materia. Asimismo, se reconocen los derechos de Acceso, Rectificación, Cancelación y Oposición (también conocidos por su acrónimo como derechos ARCO) que hacen explícito el ámbito de autodeterminación informativa del derecho a la protección de datos personales.

Posterior a la reforma de 2009 viene la reforma constitucional en materia de transparencia, publicada en el Diario Oficial de la Federación el 7 de febrero de 2014, misma que obedeció, entre otras cuestiones, a la necesidad de establecer estándares homogéneos en la protección de datos personales en toda la República Mexicana.

Precisamente la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada hasta el 26 de enero de 2017, constituye la materialización de la reforma constitucional de 2014. Por medio de ésta se desarrollan los principios, bases y procedimientos establecidos por nuestra carta magna por lo que se refiere al derecho a la protección de datos personales en posesión de los sujetos obligados. Se trata del marco jurídico general aplicable de manera directa a la Federación y a partir del cual los estados adoptan su propio régimen legal y se emiten las diversas medidas regulatorias en los distintos órdenes de gobierno.

En tales consideraciones, el Centro Nacional de Control de Energía (CENACE) como sujeto obligado y responsable en el tratamiento de datos personales que conforme a sus atribuciones lleve a cabo, garantizará la privacidad de los individuos.

Así, entre las acciones que debe realizar el CENACE como responsable del tratamiento de datos personales, y con la finalidad de cumplir con el principio de responsabilidad, se encuentra la elaboración de políticas y programas de protección de datos personales, a fin de implementar mejores prácticas al interior de la organización, por lo que, para la elaboración del presente Programa de Protección de Datos Personales, se identificaron las obligaciones que se deben cumplir y los principios que se deben observar en el tratamiento de datos personales, conforme a la etapa del ciclo de vida

de los datos personales; lo anterior, conforme a lo que establece la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGDPPSO) y demás normatividad que regula la materia, y a partir de ello, se definieron las acciones a seguir para su cumplimiento.

Finalmente, el presente Programa está basado en un sistema de gestión que permite proveer los elementos y actividades de dirección, operación y control de los procesos de la Institución, para proteger de manera sistemática y continua los datos personales que estén en su posesión, entendiendo como un 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, así como, el cumplimiento de los principios, deberes y obligaciones previstos en dicha ley y las demás disposiciones que resulten aplicables en la materia.

## **MARCO JURÍDICO.**

### **Constitución Política:**

1. Constitución Política de los Estados Unidos Mexicanos.

### **Leyes:**

1. Ley Orgánica de la Administración Pública Federal.
2. Ley Federal de las Entidades Paraestatales.
3. Ley de la Industria Eléctrica.
4. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

### **Estatuto:**

1. Estatuto Orgánico del Centro Nacional de Control de Energía.

### **Manual de Organización General:**

1. Manual de Organización General del Centro Nacional de Control de Energía.

### **Lineamientos:**

1. Acuerdo mediante el cual se aprueban los Lineamientos Generales de Protección de Datos Personales para el Sector Público.
2. Acuerdo mediante el cual se aprueban las disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales.
3. Acuerdo mediante el cual se aprueban los Parámetros de Mejores Prácticas en Materia de Protección de Datos Personales del Sector Público.
4. Acuerdo mediante el cual se aprueban los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales.
5. Acuerdo del Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, por el que se aprueban los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.
6. Acuerdo por el que se reforman los lineamientos para la Integración y Funcionamiento del Comité de Transparencia del CENACE.

## **GLOSARIO.**

**Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias y evaluarlas de manera objetiva para determinar el grado de cumplimiento de los criterios preestablecidos para la misma.

**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.

**Comité de Transparencia:** Instancia a la que hace referencia el artículo 43 de la Ley General de Transparencia y Acceso a la Información Pública, autoridad máxima en materia de protección de datos personales.

**CENACE:** Centro Nacional de Control de Energía.

**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.

**Documento de Seguridad:** El 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.

**Evaluación de impacto en la protección de datos personales:** Evaluación mediante la cual los sujetos obligados que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, valoran los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles

riesgos relacionados con los principios, deberes y derechos de los titulares, así como los deberes de los responsables y encargados, previstos en la normativa aplicable.

**Instituto o INAI:** Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

**Incidente:** Cualquier violación a las medidas de seguridad físicas, técnicas o administrativas del CENACE, que afecte la confidencialidad, la integridad o la disponibilidad de los datos personales.

**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:** El conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger la información en posesión del CENACE.

**Portabilidad de datos personales:** Prerrogativa del titular de obtener una copia de los datos que ha proporcionado al responsable del tratamiento en un formato estructurado que le permita seguir utilizándolos.

**Programa:** Programa de Protección de Datos Personales.

**Responsable del tratamiento de datos personales:** CENACE a través de sus unidades administrativas.

**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:** Combinación de la probabilidad de un evento y su consecuencia desfavorable.

**Servidor público:** El o los servidores públicos de las unidades administrativas, encargados del tratamiento de datos personales.

**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.

**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.

**Unidad Administrativa:** Las instancias del CENACE previstas en el Estatuto Orgánico y que traten o puedan tratar datos personales.

**Unidad de Transparencia:** La instancia a la que hace referencia el artículo 85 de la Ley General.

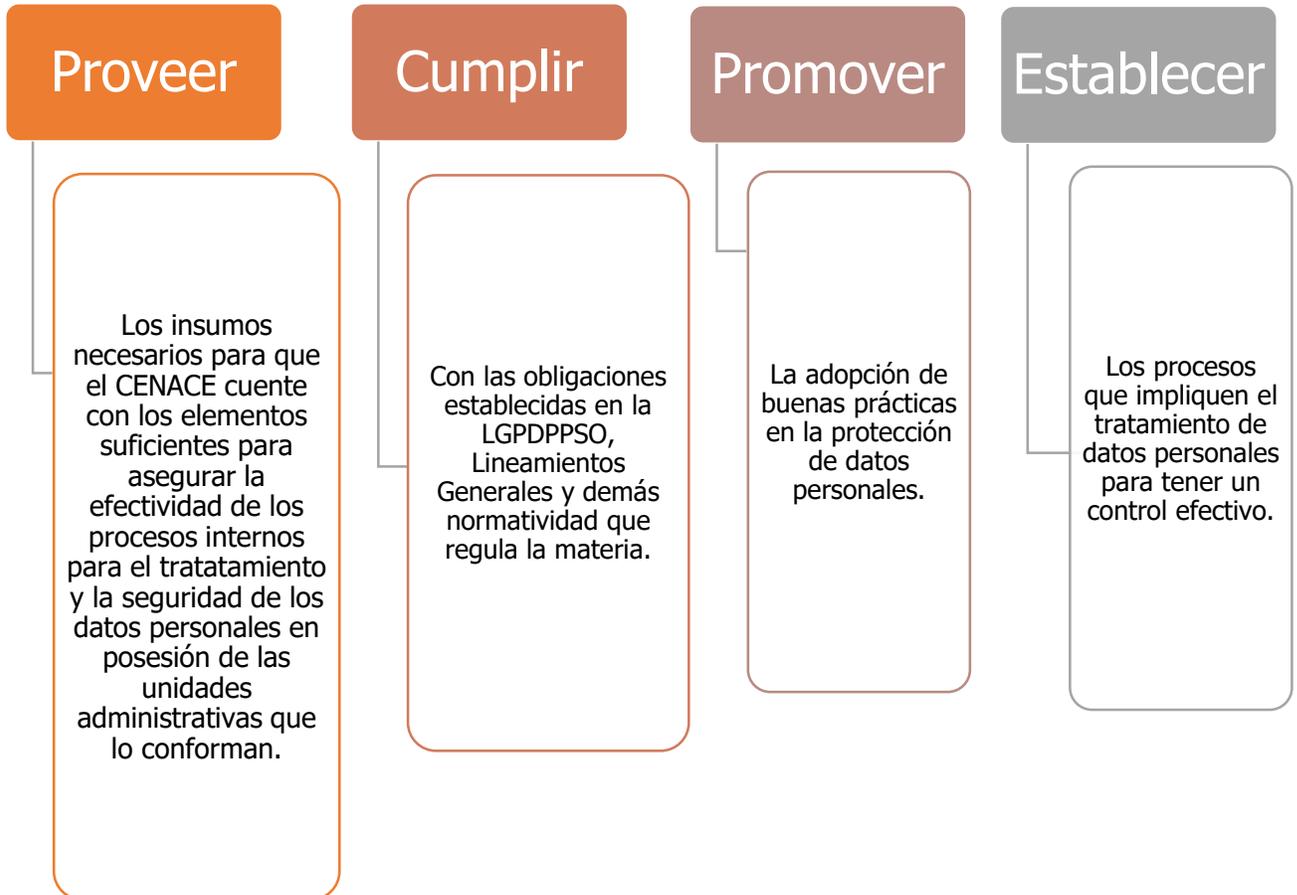
**Vulnerabilidad:** La circunstancias o condición propia de un activo, que puede ser explotada por una o más amenazas para causarle daño.

**Vulneración de seguridad:** El incidente de seguridad que afecta a los datos personales en cualquier fase de su tratamiento.

## **OBJETIVO.**

La finalidad del Programa consiste en que el CENACE garantice permanentemente que el tratamiento que realiza de los datos personales en su posesión se adecue y cumpla con los principios y obligaciones previstos en la LGPDPPSO, en los Lineamientos Generales y demás normatividad aplicable en la materia.

A efecto de lograr lo señalado, se han trazado los siguientes objetivos:



## **RESPONSABILIDADES DENTRO DEL PROGRAMA.**

De conformidad con lo dispuesto en los artículos 83 y 84, fracción I de la LGPDPPSO; 47, segundo párrafo y 48 de los Lineamientos Generales, el Comité de Transparencia es la autoridad máxima en materia de protección de datos personales, y dentro de sus funciones se encuentra el coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del CENACE.

Por ello, dicho Órgano Colegiado tendrá, en relación con este programa, las funciones siguientes:

- I.** Aprobar, coordinar y supervisar el Programa;
- II.** Proponer cambios y mejoras al Programa a partir de la experiencia de su implementación;
- III.** Dar a conocer el Programa al interior del sujeto obligado a través de la Jefatura de Unidad de Transparencia;
- IV.** Coordinar la implementación del Programa en las unidades administrativas del CENACE;
- V.** Asesorar a las áreas competentes en la implementación de este Programa con el apoyo de la Jefatura de la Unidad de Transparencia;
- VI.** Aprobar el programa anual de capacitación;
- VII.** Llevar a cabo una revisión anual de las acciones realizadas para cumplir con lo dispuesto en este Programa en el mes de abril de cada año; lo anterior, con el apoyo de la Jefatura de Unidad de Transparencia; y
- VIII.** Las demás que de manera expresa señale el propio Programa.

## **ALCANCE DEL PROGRAMA.**

El presente programa aplicará a todas las unidades administrativas que realicen tratamiento de datos personales en ejercicio de sus atribuciones, quienes además deberán de cumplir con los principios, deberes y obligaciones establecidas en la normatividad que regula la materia. Quedan exceptuados de la aplicación de este programa, los datos personales que correspondan al cumplimiento de las obligaciones de transparencia a las que refieren el artículo 120 de la Ley General de Transparencia y Acceso a la Información Pública y numeral 117 de la Ley Federal de Transparencia y Acceso a la Información Pública.

Este Programa es de observancia obligatoria para todas las personas servidoras públicas que en el ejercicio de sus funciones realicen el tratamiento de datos personales en el CENACE.

## **CUMPLIMIENTO DE OBLIGACIONES.**

Se deberán observar las siguientes:

**A. Obligaciones transversales.** Los deberes de seguridad y confidencialidad deben observarse en cualquier etapa del ciclo de vida de los datos personales. Estas obligaciones se cumplen a través de los siguientes:

**1. 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.

**2. Vulneraciones.** Se considera como vulneración las siguientes:

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

Cuando ocurra una vulneración, el CENACE debe informar al titular de los datos personales de las vulneraciones que afecten de forma significativa los derechos patrimoniales o morales, ello en cuanto se confirme que ocurrió la vulneración y siempre 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.

**3. Principios.** Se deberán observar los siguientes principios durante todas las etapas del ciclo del tratamiento de los datos personales, a saber:

**a)** Confidencialidad. Establecer controles o mecanismos para que todas las personas que intervengan en cualquier fase del tratamiento de los datos personales, guarden confidencialidad, obligación que subsistirá aún después de finalizar sus relaciones con el mismo y sin menoscabo de lo establecido en las disposiciones de acceso a la información pública.

**b)** Responsabilidad. Implementar las siguientes acciones para acreditar el cumplimiento de los principios, deberes y obligaciones, así como para rendir cuentas:

- Autorizar y destinar recursos para la instrumentación de programas y políticas de protección de datos personales.
- Elaborar políticas y programas de protección de datos personales.
- Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales.
- Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran.

- Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.
- Establecer procedimientos para recibir y responder dudas y quejas de los titulares.
- Diseñar, desarrollar e implementar las 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 la presente Ley y las demás que resulten aplicables en la materia, y
- Garantizar que las 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 LGPDPPSO, los Lineamientos Generales y las demás que resulten aplicables en la materia.

## **B. Obligaciones relevantes**

- 1.** En la etapa de obtención de los datos personales, se deben observar los siguientes principios:
  - a. Licitud.** Tratar los datos personales que posea el CENACE sujetándose a las atribuciones o facultades de la normatividad aplicable.
  - b. Lealtad.** Obtener los datos sin dolo, mala fe, engaño o negligencia.
  - c. Información.** Poner a disposición del titular el aviso de privacidad al momento de la obtención de los datos personales. Difundir el aviso de privacidad por medios electrónicos y físicos. El aviso de privacidad deberá estar redactado conforme a la normatividad en materia de datos personales, para sus dos versiones integral y simplificado.
  - d. Consentimiento.** Contar con el consentimiento del titular, para el tratamiento de sus datos personales, salvo que se actualice alguna de las excepciones previstas en el artículo 22 (excepciones para la obtención del consentimiento) de la LGPDPPSO. (Se debe considerar: Consentimiento menores de edad y personas en estado de interdicción o incapacidad declarada conforme a la Ley). Para este principio resulta importante resaltar que no se deben tratar datos personales sensibles salvo que se cuente con el consentimiento expreso del titular o se trate de los casos establecidos en el artículo 22 de la LGPDPPSO.
  - e. Proporcionalidad.** Tratar los datos personales sólo cuando resulten adecuados, relevantes y necesarios para la finalidad que justifica su tratamiento. Se entenderá que los datos personales son adecuados, relevantes y estrictamente necesarios cuando son apropiados, indispensables y no excesivos para el cumplimiento de las finalidades que motivaron su obtención.
- 2.** En la etapa de uso de los datos personales, se deben observar los siguientes principios:
  - a. Finalidad.** Justificar el tratamiento de los datos personales en finalidades concretas, lícitas, explícitas y legítimas. Se entenderá que las finalidades son:

- Concretas: cuando el tratamiento de los datos personales atiende a la consecución de fines específicos o determinados, sin que admitan errores, distintas interpretaciones o provoquen incertidumbre, dudas o confusión en el titular.
- Explícitas: cuando las finalidades se expresan y dan a conocer de manera clara en el aviso de privacidad.
- Lícitas: cuando las finalidades que justifican el tratamiento de los datos personales son acordes con las atribuciones o facultades de la Unidad Administrativa que corresponda.
- Legítimas: cuando las finalidades que motivan el tratamiento de los datos personales se encuentren habilitadas por el consentimiento del titular, salvo que se actualice alguna de las causales de excepción previstas en el artículo 22 de la Ley General.

**b. Calidad.** Adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales, principalmente cuando se obtuvieron de manera indirecta del titular. Se entenderá que los datos personales son:

- Exactos y correctos: cuando los datos personales en posesión del responsable no presentan errores que pudieran afectar su veracidad.
- Completos: cuando su integridad permite el cumplimiento de las finalidades que motivaron su tratamiento y de las atribuciones del responsable.
- Actualizados: cuando los datos personales responden fielmente a la situación actual del titular.

**3.** En la etapa de eliminación de los datos personales, se deben observar los siguientes principios:

**a. Supresión de datos personales.** Suprimir los datos personales cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades y una vez que concluya su plazo de conservación establecido.

## **FUNCIONES DEL COMITÉ DE TRANSPARENCIA.**

El Comité de Transparencia será la autoridad máxima en materia de protección de datos personales al interior del CENACE, y al respecto, tendrá las siguientes funciones:

- I.** Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en el CENACE, de conformidad con las disposiciones previstas en la LGPDPPSO y en aquellas disposiciones que resulten aplicables en la materia;
- II.** Instituir, en su caso, procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO;
- III.** 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;
- IV.** Establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor observancia de la LGPDPPSO y en aquellas disposiciones que resulten aplicables en la materia;
- V.** Supervisar, en coordinación con las unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad;
- VI.** Dar seguimiento y cumplimiento a las resoluciones emitidas por el INAI;
- VII.** Establecer programas de capacitación y actualización para los servidores públicos en materia de protección de datos personales, y
- VIII.** 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 las unidades administrativas.

## **FUNCIONES DE LA UNIDAD DE TRANSPARENCIA.**

La Unidad de Transparencia tendrá las siguientes funciones en materia de protección de datos personales:

- I.** Auxiliar y orientar al titular que lo requiera con relación al ejercicio del derecho a la protección de datos personales;
- II.** Gestionar las solicitudes para el ejercicio de los derechos ARCO;
- III.** Establecer mecanismos para asegurar que los datos personales solo se entreguen a su titular o su representante debidamente acreditados;
- IV.** 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;
- V.** 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;
- VI.** Aplicar instrumentos de evaluación de calidad sobre la gestión de las solicitudes para el ejercicio de los derechos ARCO, y
- VII.** Asesorar a las unidades administrativas en materia de protección de datos personales.

## **CAPACITACIÓN.**

Se establecerá un programa anual de capacitación y actualización en materia de protección de datos personales, dirigido tanto a personal como a encargados. El programa de capacitación deberá ser a corto, mediano y largo plazo y considerar los roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales y el perfil de puestos.

## **REVISIONES Y AUDITORIAS.**

Se deberá de contar con un programa para llevar a cabo dos tipos de acciones: 1) auditorías y 2) revisiones administrativas. Las revisiones administrativas las realizará el propio Comité con el apoyo de la Jefatura de Unidad de Transparencia, mientras que las auditorías las deberá realizar un actor externo al Comité de Transparencia, pudiendo ser: 1. Externas, cuando exista el presupuesto para ello y la importancia del caso lo amerite, o 2. Voluntarias, realizadas a través del INAI conforme a lo que señala el artículo 151 de la LGPDPPSO.

## **LA DEFINICIÓN DE ACCIONES PARA LA MEJORA CONTINUA.**

El proceso de revisión y mejora continua permitirá verificar que los parámetros establecidos en la LGPDPPSO, en los Lineamientos Generales, en este Programa de Protección de Datos Personales y en el Documento de Seguridad y demás normatividad aplicable de la que deriven obligaciones en materia de protección de Datos Personales se cumplan estrictamente o permitan realizar los ajustes necesarios para su cumplimiento y perfeccionamiento.

Con lo anterior se permitirá garantizar el tratamiento óptimo de los datos personales en posesión del CENACE.

En ese sentido, la Jefatura de Unidad de Transparencia, por sí o a petición de las instancias, dará cuenta al Comité de Transparencia de los puntos de mejora en materia de protección de datos personales que hayan sido advertidos de las auditorías y/o revisiones internas realizadas, así como de aquellos eventos derivados del Documento de Seguridad para la Protección de Datos Personales del CENACE, particularmente de los indicados en los capítulos III –Del contenido y actualización del documento de seguridad-, IV –De los mecanismos de monitoreo y revisión de las medidas de seguridad- y IX – De los incidentes y vulneraciones a la seguridad-; o bien, de aquellas circunstancias que se estimen relevantes o de inmediata aplicación para perfeccionar las directrices incluidas en este Programa.

El Comité de Transparencia por sí o a través de la Jefatura de Unidad de Transparencia realizará las recomendaciones que estime conveniente en materia de protección de datos personales, teniendo como finalidad fundamental que las unidades administrativas adopten acciones preventivas y correctivas, debiendo documentar los resultados y revisiones de los puntos de mejora desarrollados.

## **SANCIONES.**

De manera enunciativa más no limitativa son causa de sanción de las obligaciones establecidas en la Ley General, las señaladas en el artículo 163 de dicho ordenamiento Jurídico, el cual se cita para pronta referencia:

**Artículo 163.** Serán causas de sanción por incumplimiento de las obligaciones establecidas en la materia de la presente Ley, 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 presente Ley 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 en la presente Ley;
- 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 presente Ley, 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 establecido en el artículo 42 de la presente Ley;
- VIII.** No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la presente Ley;
- 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 presente Ley;
- X.** Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la presente Ley;
- XI.** Obstruir los actos de verificación de la autoridad;
- XII.** Crear bases de datos personales en contravención a lo dispuesto por el artículo 5 de la presente Ley;
- XIII.** No acatar las resoluciones emitidas por el Instituto y los Organismos garantes, y
- XIV.** Omitir la entrega del informe anual y demás informes a que se refiere el artículo 44, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, o bien, entregar el mismo de manera extemporánea.

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

En caso de que la presunta infracción hubiere sido cometida por algún integrante de un partido político, la investigación y, en su caso, sanción, corresponderán a la autoridad electoral competente.

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

En cuanto al procedimiento que se seguirá para que se determinen las sanciones en caso de incumplimiento a los supuestos referidos previamente, se estará a lo dispuesto en el documento denominado "Políticas Internas de Gestión y Tratamiento de Datos Personales".