CENACE®

CENTRO NACIONAL DE CONTROL DE ENERGÍA

SISTEMAS DE SUPERVISIÓN Y VIGILANCIA.

Contenido

OBJETIVO.

Dar cumplimiento al artículo 30, fracciones IV y V de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; así como del artículo 49 de los *Lineamientos Generales de Protección de Datos Personales para el Sector Público;* que señalan que en atención al principio de *responsabilidad* los Sujetos Obligados deben establecer sistemas de supervisión y vigilancia interna y/o externa, incluyendo auditorías.

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.

LGPDPPSO: 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.

AMBITO DE APLICACIÓN.

Las directrices contenidas en el presente documento son de aplicación general para las personas servidoras públicas que integran las unidades administrativas adscritas al CENACE 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.

DISPOSICIONES GENERALES.

A fin de corroborar el cumplimiento del programa y de las políticas de protección de datos personales, los tratamientos de datos personales, la verificación, la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados por el CENACE para el cumplimiento de las obligaciones previstas en la LGPDPPSO; así como en los Lineamientos Generales y demás normatividad aplicable en la materia, se establecen los siguientes mecanismos:

REVISIONES EXTERNAS.

1. En cualquier momento el CENACE podrá remitir al INAI una solicitud de auditoría voluntaria, a fin de que dentro del ámbito de sus facultades y atribuciones verifique el cumplimiento de las obligaciones previstas en la LGPDPPSO; así como en los Lineamientos Generales y demás normatividad aplicable en la materia.

2. La solicitud de auditoría voluntaria se realizará al INAI mediante oficio o cualquier otro medio habilitado para tal efecto, por conducto de la Jefatura de Unidad de Transparencia previa autorización del Comité de Transparencia del CENACE.

3. La solicitud de auditoría debe contar con al menos los siguientes elementos:

- **a.** La denominación del sujeto obligado y domicilio;
- **b.** Las personas autorizadas para oír y recibir notificaciones;
- **c.** La descripción de las obligaciones en materia de protección de datos personales o, en su caso, del tratamiento de datos personales que se pretenden someter a una auditoría voluntaria, indicando, de manera enunciativa más no limitativa, las finalidades de éste; el tipo de datos personales tratados; las categorías de titulares involucrados; las transferencias que, en su caso se realicen; las medidas de seguridad implementadas; la tecnología utilizada, así como cualquier otra información relevante del tratamiento;
- **d.** Las circunstancias o razones que motivan al CENACE a someterse a una auditoría voluntaria;
- **e.** El nombre, cargo y firma del servidor público que solicita la auditoría, y
- **f.** Cualquier otra información o documentación que se considere relevante hacer del conocimiento del INAI.

4. Durante el desarrollo de la auditoria voluntaria, las unidades administrativas y servidores públicos involucrados, en todo momento deberán:

- **a.** Proporcionar y mantener a disposición de los auditores autorizados por el INAI la información, documentación o datos relacionados con el tratamiento de datos personales objeto de la auditoria voluntaria;
- **b.** Permitir y facilitar a los auditores autorizados del Instituto el acceso a archiveros, registros, archivos, sistemas, equipos de cómputo, discos o cualquier otro medio o sistema de tratamiento de los datos personales objeto de la auditoria voluntaria;
- **c.** Permitir el acceso a los auditores autorizados por el Instituto al lugar, a las oficinas o instalaciones del CENACE donde se lleve a cabo el tratamiento de datos personales auditado;
- **d.** Asistir a las reuniones que se programen para los efectos de la auditoría, y
- **e.** Desahogar los requerimientos realizados por el INAI en los plazos y términos que fije.

5. Concluida la auditoria voluntaria, el INAI emitirá un informe final en el cual señalará los resultados obtenidos de la auditoría y se pronunciará sobre la conformidad o no conformidad de los controles, mecanismos o procedimientos adoptados por el responsable auditado para el cumplimiento de las obligaciones previstas en la LGPDPPSO; así como en los Lineamientos Generales y demás normatividad aplicable en la materia.

6. El informe final que emita el INAI orientará al CENACE sobre el fortalecimiento y un mejor cumplimiento de las obligaciones previstas en normatividad aplicable, pudiendo señalar medidas, acciones, recomendaciones y sugerencias específicas de carácter preventivo y/o correctivo que deben ser atendidas, en función de las características generales y particularidades del tratamiento de datos personales y de los hallazgos obtenidos en la auditoria.

7. El CENACE deberá informar al INAI sobre la implementación de las recomendaciones emitidas en el informe final en los plazos que se fijen para tal efecto.

8. Se podrán solicitar auditorías a entes externos especializados y certificados en protección de datos personales, siempre que exista presupuesto para su contratación y a consideración del Comité de Transparencia las circunstancias del caso en particular lo ameriten.

REVISIONES INTERNAS.

1. En cualquier momento el Comité de Transparencia podrá proponer la realización de una supervisión interna a las unidades administrativas con el objeto de comprobar el cumplimiento de las obligaciones previstas en la LGPDPPSO; así como en los Lineamientos Generales y demás normatividad aplicable en la materia.

2. Las revisiones que apruebe el Comité de Transparencia se ajustaran a las siguientes etapas:

- **a.** Antecedentes;
- **b.** Objetivo, periodo y lugar;
- **c.** Resultado de las observaciones realizadas;
- **d.** Conclusión y recomendaciones generales, y
- **e.** Seguimiento

3. El proceso de revisión permitirá verificar que los parámetros establecidos en la LGPDPPSO, en los Lineamientos Generales se cumplan cabalmente o permitan realizar los ajustes necesarios para su cumplimiento.

4. La finalidad de la implementación de las revisiones permitirá garantizar el tratamiento óptimo de los datos personales en posesión del CENACE, y así determinar las medidas preventivas y/o correctivas a seguir, para mejorar los mecanismos, términos y procedimientos en la materia de que se trate.

5. El proceso de revisión se efectuará por el personal designado por el Comité de Transparencia.

6. Durante el desarrollo de la revisión, las unidades administrativas y servidores públicos involucrados, en todo momento deberán:

- **a.** Proporcionar y mantener a disposición del personal autorizado la información, documentación o datos relacionados con el tratamiento de datos personales objeto de la revisión;
- **b.** Permitir y facilitar al personal autorizado el acceso a archiveros, registros, archivos, sistemas, equipos de cómputo, discos o cualquier otro medio o sistema de tratamiento de los datos personales objeto de la revisión;
- **c.** Permitir el acceso al personal autorizado al lugar, a las oficinas o instalaciones del CENACE donde se lleve a cabo el tratamiento de datos personales auditado;
- **d.** Asistir a las reuniones que se programen para los efectos de la auditoría, y
- **e.** Desahogar los requerimientos realizados por el personal autorizado en los plazos y términos que fije.

7. El Comité de Transparencia establecerá un plazo límite para que se corrijan las inconformidades detectadas, situación que deberá quedar debidamente documentada.

8. Se deberá informar al Comité de Transparencia por parte de las unidades administrativas revisadas, sobre la implementación de las recomendaciones emitidas en los plazos que se fijen para tal efecto.