Programa de Protección de Datos Personales del Centro Nacional de Prevención de Desastres (CENAPRED)

Unidad de Transparencia

Abril 2022

Programa de Protección de Datos Personales

1. Objetivos del Programa

1. Proveer el marco de trabajo necesario para la protección de los datos personales en posesión del Centro Nacional de Prevención de Desastres (CENAPRED);
2. Cumplir con las obligaciones que establece la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y los Lineamientos Generales, así como la normatividad que derive de los mismos,
3. Establecer los elementos y actividades de dirección, operación y control de los procesos que impliquen el tratamiento de datos personales, a efecto de protegerlos de manera sistemática y continua.

2. Responsabilidades dentro del Programa

Con fundamento en lo dispuesto por los artículos 83 y 84, fracción I de la LGPDPPSO y 47, segundo párrafo, y 48 de los Lineamientos Generales, que señalan que el Comité de Transparencia es la autoridad máxima en materia de protección de datos personales y que tiene entre sus funciones la de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, dicho órgano tendrá las siguientes funciones con relación a este programa:

I. Elaborar, aprobar, coordinar y supervisar el Programa, en conjunto con las áreas técnicas que estime necesario involucrar o consultar;

II. Dar a conocer el Programa al interior del CENAPRED;

III. Coordinar la implementación del Programa en las unidades administrativas del sujeto obligado;

IV. Asesorar a las unidades administrativas en la implementación de este Programa, con el apoyo de las áreas técnicas que estime pertinente;

V. Supervisar la correcta implementación del Programa;

VI. Las demás que de manera expresa señale el propio Programa.

El presente Programa se deberá hacer del conocimiento del Director General del CENAPRED, a fin de que tome las medidas necesarias para que el mismo se observe en el Centro Nacional.

La intervención del Director General del CENAPRED tendrá la finalidad única de impulsar la debida implementación del Programa al interior del Centro Nacional, pero no podrá suplir ni afectar las funciones que otorgan los artículos 83 y 84 de la LGPDPPSO al Comité de Transparencia, en su carácter de máxima autoridad de datos personales en el CENAPRED.

Asimismo, para que la implementación del Programa tenga como resultado el cumplimiento integral de las obligaciones que establece la LGPDPPSO y los Lineamientos Generales, el Programa será de observancia obligatoria para todos los servidores públicos del CENAPRED que en el ejercicio de sus funciones traten datos personales.

Las unidades administrativas del CENAPRED deberán realizar las acciones necesarias para cumplir con las obligaciones que establece este Programa, para lo cual deberán asignar los recursos

materiales y humanos necesarios, y prever lo que se requiera en sus programas de trabajo.

Las unidades administrativas y la Unidad de Transparencia tendrán las funciones y responsabilidades que se describen en la sección 4 de este programa

Para ello, resulta fundamental que el Programa se conozca al interior, por lo que el Comité de Transparencia se encargará de difundirlo entre las personas servidoras públicas adscritas al CENAPRED.

Cuando los recursos humanos y presupuestales lo permitan, se sugiere que el CENAPRED cuente con el Oficial de Protección de Datos al que refiere el segundo párrafo del artículo 85 de la LGPDPPSO, que tendrá las funciones que señala ese artículo y el 121 y 122 de los Lineamientos Generales.

En caso que no se requiera el Oficial o no se cuente con los recursos para su designación, se sugiere valorar la posibilidad de designar a personal que asista al Comité de Transparencia y a la Unidad de Transparencia en el cumplimiento de sus obligaciones en materia de protección de datos personales, el cual deberá contar con conocimientos técnicos sobre el derecho de protección de datos personales.

3. Alcance del Programa

El presente Programa aplicará a todas las unidades administrativas del CENAPRED que realicen tratamiento de datos personales en ejercicio de sus atribuciones y en el desempeño de sus funciones.

Asimismo, en virtud de que uno de los objetivos del Programa es cumplir con las obligaciones establecidas en la LGPDPPSO, se cubrirán todos los principios, deberes y obligaciones que establece dicha norma para los responsables del tratamiento; con excepción en este momento por razones presupuestales y de falta de personal de las evaluaciones de impacto en la protección de datos personales, de las revisiones y auditorías a realizar y acciones de mejora continua.

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.

Las unidades administrativas que forman parte del CENAPRED a la fecha de aprobación del presente Programa, y que deberán observarlo de conformidad con el Manual de Organización Específico, Órgano Desconcentrado Administrativo, Centro Nacional de Prevención de Desastres, del 15 de julio de 2021, son las siguientes:

I. Dirección General del Centro Nacional de Prevención de Desastres

1.1 Dirección de Investigación

1.1.1 Subdirección de Riesgos Volcánicos

1.1.1.1 Departamento de Vulcanología

1.1.1.2 Departamento de Análisis y Metodologías para Riesgos Volcánicos

1.1.2 Subdirección de Dinámica de Suelos y Procesos Gravitacionales

1.1.2.1 Departamento de Análisis de Fenómenos Geotécnicos

1.1.2.2 Departamento de Análisis y Procesos Gravitacionales

Programa de Protección de Datos Personales

1.1.3 Subdirección de Riesgos Sísmicos

1.1.3.1 Departamento de Investigación Aplicada a Riesgos Sísmicos

1.1.3.2 Departamento de Análisis y Metodologías para Riesgos Geológicos

1.1.4 Subdirección de Riesgos Estructurales

1.1.4.1 Departamento de Normatividad *y* Asesoría Institucional

1.1.4.2 Departamento de Infraestructura par a la Prevención de Desastres

1.1.5 Subdirección de Vulnerabilidad Estructural

1.1.5.1 Departamento de Seguridad Estructural

1.1.0.1 Departamento de Vulnerabilidad Estructura l

1.1.0.2 Departamento de Ingeniería Sísmica y Mecánica Estructural

1.1.6 Subdirección de Riesgos por Inundación

1.1.6.1 Departamento de Riesgos por Inundación *y* Modelos Hidráulicos

1.1.6.2 Departamento de Análisis de Escenarios por Inundación

1.1.7 Subdirección de Riesgos por Fenómenos Hidrometeorológicos

1.1.7.1 Departamento de Análisis y Alertamiento Hidrometeorológico

1.1.7.2 Departamento de Sistemas de Información Hidrometeorológica

1.1.7.3 Departamento de Fenómenos Hidrometeorológicos Extremos

1.2 Dirección de Instrumentación y Cómputo

1.2.1 Subdirección de Instrumentación y Comunicaciones

1.2.1.1 Departamento de Instrumentación Volcánica

1.2.1.2 Departamento de Desarrollo e Innovación Tecnológica para la Prevención de Desastres

1.2.1.3 Departamento de Instrumentación Sísmica

1.2.1.4 Departamento de Instrumentación Hidrometereológica

1.2.2 Subdirección de Monitoreo

1.2.2.1 Departamento de Procesamiento de Datos

1.2.2.2 Departamento de Monitoreo de Fenómenos Naturales

1.2.3 Subdirección de Servicios Informáticos

1.2.3.1 Departamento de Soporte Técnico

1.2.3.2 Departamento de Desarrollo de Sistemas

1.2.3.3 Departamento de Redes y Enlaces Digitales

1.2.3.4 Departamento de Seguridad y Enlaces Digitales

Programa de Protección de Datos Personales

1.3 Dirección de la Escuela Nacional de Protección Civil

1.3.1 Subdirección de Capacitación del PERE

1.3.1.1 Departamento de Implementación y Evaluación de Capacitación del PERE

1.3.1.2 Departamento de Diseño *y* Desarrollo de Capacitación del PERE

1.3.2 Subdirección de Acreditación y Certificación de Competencia

1.3.2.1 Departamento de Acreditación y Certificación del Sistema Escolarizado

1.3.2.2 Departamento de Acreditación y Certificación del Sistema de Competencias

1.3.3 Subdirección de Gestión Educativa

1.3.3.1 Departamento de Gestión Educativa del Sistema de Competencias

1.3.4 Subdirección de Coordinación Interinstitucional de Protección Civil

1.3.5 Subdirección de Capacitación en Protección Civil

1.3.5.1 Departamento de Capacitación en Protección Civil

1.3.5.2 Departamento de Implementación de Estrategias Didácticas y Educativas

1.3.5.3 Departamento de Logística y Planeación de Cursos

1.3.5.4 Departamento de Diseño y Desarrollo de Estrategias Didácticas y Educativas

1.4 Dirección de Análisis y Gestión de Riesgos

1.4.1 Subdirección de Riesgos Químicos

1.4.1.1 Departamento de Análisis y Sustancias Peligrosas

1.4.1.2 Departamento de Riesgos Químicos en Almacenamiento, Transporte y Distribución

1.4.2 Subdirección de Riesgos Sanitarios y Toxicología

1.4.2.1 Departamento de Riesgos Sanitarios y Toxicología

1.4.2.2 Departamento de Laboratorio de Riesgos Sanitarios

1.4.3 Subdirección de FOPREDEN

1.4.3.1 Departamento de Supervisión y Evaluación de Proyectos

1.4.4 Subdirección de Sistemas de Información sobre Riesgos

1.4.4.1 Departamento de Sistemas de Información sobre Riesgos

1.4.4.2 Departamento de Administración de Sistemas Geoespaciales

1.4.5 Subdirección de Coordinación, Evaluación y Diseño de Políticas Públicas para la Prevención de Desastres

1.4.5.1 Departamento de Análisis y Diseño de Políticas Públicas para la Prevención de Desastres

1.4.5.2 Departamento de Evaluación y Seguimiento de Políticas Públicas para la Prevención de Desastres

1.4.6 Subdirección de Estudios Económicos y Sociales sobre Desastres

1.4.6.1 Departamento de Estudios Económ1cos y Sociales sobre Desastres

Programa de Protección de Datos Personales

1.5 Coordinación de Políticas Públicas para la Prevención de Desastres

1.6 Dirección de Difusión
1.6.1 Subdirección de Promoción Cultural
1.6.1.1 Departamento de Diseño y Logística
1.6.1.2 Departamento de Campañas
1.6.2 Subdirección de Editorial y Publicaciones
1.6.2.1 Departamento de Servicios Editoriales
1.6.2.2 Departamento de Análisis de Contenido
1.6.2.3 Departamento de Documentación y Medios
1.6.2.4 Departamento *de* Medios y Redes

1.7 Dirección de Servicios Técnicos
1.7.1 Subdirección de Asuntos Nacionales e Internacionales
1.7.1.1 Departamento de Asuntos Nacionales
1.7.2 Subdirección Jurídica
1.7.2.1 Departamento Jurídico

1.8 Coordinación Administrativa
1.8.1 Subdirección de Recursos Materiales y Servicios Generales
1.8.1.1 Departamento de Compras y Servicios Generales
1.8.1.2 Departamento de Inventarios y Archivo
1.8.2 Subdirección de Recursos Financieros
1.8.2.1 Departamento de Recursos Financieros
1.8.3 Subdirección de Recursos Humanos
1.8.3.1 Departamento de Organización y Control de Plazas

1.0.1 Subdirección de Vinculación y Gestión Institucional
1.0.1.1 Departamento de Enlace Institucional
1.0.1.2 Departamento de Control de Gestión
1.0.0.1 Departamento de Apoyo y Enlace Institucional

Programa de Protección de Datos Personales

4. Política de Gestión de los Datos Personales

En observancia a lo dispuesto por los artículos 47 y 56 de los Lineamientos Generales en relación con lo dispuesto por la Política Interna de Protección de Datos Personales del CENAPRED, en todos los tratamientos de datos personales que realicen las unidades administrativas, se deberá observar y cumplir lo establecido por la LGPDPPSO y los Lineamientos Generales, protegiendo de una manera sistemática y continua y según el ciclo de vida de los datos personales de conformidad con el Catálogo de Disposición Documental Común de la Secretaría de Seguridad y Protección Ciudadana.

El CENAPRED procurará la adopción de mejores prácticas para la protección de datos personales, en aquellos tratamientos que así lo permitan de acuerdo a la disponibilidad presupuestal, así como a la asignación de recursos humanos y materiales con los que cuente.

4.1 Inventario de tratamientos de datos personales

Cada una de las unidades administrativas realizará un diagnóstico de los tratamientos de datos personales que llevan a cabo.

El diagnóstico tendrá como base la elaboración de un inventario con la información básica de cada tratamiento de datos personales que se realizan en el CENAPRED.

Por "inventario de tratamientos de datos personales" se entenderá el control documentado que se llevará de los tratamientos que realizan las unidades administrativas del CENAPRED, realizado con orden y precisión.

El inventario de datos personales al que hace referencia la LGPDPPSO en los artículos 33, fracción III, 35, fracción I, y 58 de los Lineamientos Generales, identificará los siguientes elementos relevantes:

1.- Se deberá identificar cada uno de los procesos en los que cada una de las unidades administrativas trata datos personales.

Tratar datos personales es un concepto amplio, que incluye: cualquier operación u operaciones realizadas mediante procedimientos manuales o automatizados, relacionados con las siguientes acciones:

Obtención Uso Registro Organización Conservación Elaboración	Utilización Comunicación Difusión Almacenamiento Posesión Acceso	Manejo Aprovechamiento Divulgación Transferencia Disposición

2.- La Unidad Administrativa del CENAPRED encargada, de ser la administradora de las bases de datos o archivos que se generen con motivo del tratamiento de datos personales, será aquella qué este a cargo y sea responsable del procedimiento específico de acuerdo con las atribuciones o

funciones encomendadas en el Manual de Organización Específico[1].

3.- En caso en que dos o más unidades administrativas estén a cargo de un proceso mediante el cual se recaban los datos personales y que administren las bases de datos correspondientes de manera conjunta.

4.- La Unidad administrativa responsable será quien decida sobre el tratamiento de los datos personales, es decir, quien establece las finalidades del tratamiento o el uso que se le dará a los datos personales, el tipo de datos que se requieren, a quién y para qué se comparten, cómo se obtienen, almacenan y suprimen los datos personales, y en qué casos se divulgarán, entre otros factores de decisión.

5.-Una vez identificados los tratamientos de los cuales está a cargo, cada unidad administrativa, determinará lo siguiente, de acuerdo con el ciclo de vida de los datos personales:

5.1.- ¿Cómo se obtienen los datos personales?

Los datos personales se pueden obtener de tres formas:

a) De forma personal.- Cuando el titular proporciona los datos personales al responsable o a la persona física designada por el responsable, con la presencia física de ambos. Por ejemplo, cuando el titular acude a un hospital público (responsable) y ahí mismo proporciona sus datos personales;

b) De manera directa.- Cuando el titular proporciona los datos personales por algún medio que permite su entrega directa al responsable, entre ellos, medios electrónicos, ópticos, sonoros, visuales o cualquier otra tecnología, como correo postal, Internet o vía electrónica, entre otros.

Por ejemplo, cuando el titular envía sus datos por correo electrónico o cuando los comunica vía telefónica al responsable; o bien,

c) De manera indirecta.- Cuando el responsable obtiene los datos personales sin que el titular se los haya proporcionado de forma personal o directa, como podría ser a través de transferencias o fuentes de acceso público.

5.2- ¿Qué tipo de datos personales se tratan? ¿Son sensibles?

5.3.- ¿Dónde se almacenan y realiza el tratamiento de los datos personales?

- Sección, serie y subserie de archivos
- Formato en que se encuentra la base de datos: físico y/o electrónico
- Ubicación de la base de datos

5.4.- ¿Para qué finalidades se utilizan los datos personales?

Las finalidades son acciones más específicas de los procesos o procedimientos de los que derivan los tratamientos de datos personales.

Será necesario identificar si se requiere el consentimiento o no de los titulares y el tipo de consentimiento (tácito o expreso y por escrito), y en caso de que no se requiera, definir qué supuestos

[1] Por ejemplo, con motivo de una consulta, la unidad administrativa "X" podría tener acceso a datos de contacto del particular que realizó la consulta, sin embargo, la unidad administrativa que está a cargo del procedimiento de atención a consultas, y quien administra la base de datos de las consultas que recibe la institución es la unidad administrativa "Y".

(fracciones) del artículo 22 de la LGPDPPSO se actualizan.

Se deberá señalar el marco jurídico que da facultades para el tratamiento de datos personales (disposición normativa, artículo, fracción, inciso, párrafo).

5.5. ¿Quién tiene acceso a la base de datos o archivos (sistemas de tratamiento) y a quién se comunican los datos personales al interior del CENAPRED?

Se deberá identificar el catálogo de personas servidoras públicas al interior del CENAPRED que tienen acceso a los datos personales y para qué fin.

5.6. ¿Intervienen encargados en el tratamiento de los datos personales?

Es necesario identificar el nombre del encargado y el número de contrato, pedido o convenio correspondiente.

5.7. ¿Qué transferencias se realizan o se podrían realizar de los datos personales y con qué finalidad?

Las Unidades Administrativas del CENAPRED deberán identificar las autoridades o terceros externos a nombre del CENAPRED, a quienes se comunican los datos personales y los fines de las transferencias.

Será necesario identificar si se requiere el consentimiento para la transferencia, el tipo de consentimiento que se requiere en su caso (tácito o expreso y por escrito), y en caso de que no se requiera el consentimiento, se deberá definir qué supuestos (fracciones) de los artículos 22, 66 o 70 de la LGPDPPSO se actualizan.

5.8. ¿Se difunden los datos personales?

Las Unidades Administrativas del CENAPRED deberán señalar si los datos personales se difunden y el fundamento jurídico para ello.

5.9.- ¿Cuál es el plazo de conservación de los datos personales?

Este plazo deberá ser definido de acuerdo a lo señalado en el Catálogo de Disposición Documental Común de la Secretaría de Seguridad y Protección Ciudadana, por lo que es necesario identificar a qué serie documental pertenecen los archivos o bases de datos en los que están contenidos los datos personales.

El diagnóstico se deberá realizar conforme a la matriz de **Anexo 1** de este Programa (Inventario de Tratamientos), y se deberá realizar por proceso, procedimiento o Unidad administrativa, según aplique el caso.

4.2 Cumplimiento de Obligaciones

En la presente sección se identificarán las obligaciones que establecen la LGPDPPSO y los Lineamientos Generales y se dividirán según las distintas etapas del ciclo de vida de los datos personales (obtención, uso y eliminación).

Si bien, las obligaciones se dividieron según el ciclo de vida de los datos personales, es importante señalar que es ineludible cumplir con todos los principios y deberes que establecen la LGPDPPSO, los Lineamientos Generales y demás normatividad que resulte aplicable, en cualquier momento del tratamiento o ciclo de vida de los datos personales.

4.2.1. Obligaciones Transversales (T)

Las Unidades Administrativas del CENAPRED, cumplirán con los deberes de seguridad y confidencialidad en cualquier etapa del ciclo de vida de los datos personales y atendiendo en todo momento a lo establecido en la Política Interna de Protección de Datos Personales en relación con lo previsto en la Política de Seguridad en Datos Personales, ambos documentos emitidos y aplicables al CENAPRED.

Por lo que en el presente programa solo se enlistarán de manera enunciativa más no limitativa:

- Medidas de Seguridad
- Documento de Seguridad
- Vulneraciones
- Confidencialidad

Para el efectivo cumplimiento de este apartado, las Unidades Administrativas del CENAPRED deberán utilizar como referencia el contenido del **Anexo 2 y 3**, de este Programa.

4.2.2. Obligaciones relevantes en la etapa de OBTENCIÓN de los datos personales. (O)

Las Unidades Administrativas del CENAPRED, para el cumplimiento de las obligaciones relevantes en la etapa de la Obtención (O) deberán atender en todo momento a lo establecido en la Política Interna de Protección de Datos Personales en el CENAPRED así como en lo dispuesto en los Criterios para la Elaboración de Avisos de Privacidad ambos documentos del CENAPRED, destacándose lo siguiente:

1.O. LICITUD

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
Sujetar el tratamiento de los datos personales a las atribuciones o facultades que la normatividad aplicable confiera al CENAPRED, así como con estricto apego y cumplimiento de lo dispuesto en dicho ordenamiento, los Lineamientos Generales, la legislación mexicana que le resulte aplicable y, en su caso, el derecho internacional, respetando los derechos y libertades de los	1. Identificar el marco normativo (leyes, tratados o acuerdos internacionales, reglamentos, lineamientos, entre otros, con sus respectivos artículos) que faculta a la unidad administrativa a tratar los datos personales para cada una de las finalidades, y aquél que regula el tratamiento respectivo.	Todas las unidades administrativas que realicen tratamiento de datos personales.	Marco normativo respectivo.

Programa de Protección de Datos Personales

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
titulares.			

Artículos vinculados: 17 de la LGPDPPSO y 8 de los Lineamientos Generales.

Comprobación:	Sí	No
1. Están identificadas las disposiciones normativas (ley, acuerdos o tratados internacionales, reglamentos, lineamientos, entre otros, con sus respectivos artículos) que facultan a la unidad administrativa a tratar los datos personales para cada una de las finalidades que lleva a cabo, y aquél que regula el tratamiento respectivo.	☐	☐

2.O. LEALTAD

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
No obtener ni tratar los datos personales a través de medios engañosos o fraudulentos. De acuerdo con el artículo 11, fracción I, de los Lineamientos Generales, se entiende por medios engañosos y fraudulentos aquéllos que se utilicen para tratar los datos personales con dolo, mala fe o negligencia.	1. Verificar que los datos personales no se obtengan con dolo, mala fe o negligencia.	Todas las unidades administrativas que realicen tratamiento de datos personales.	• Medios para la obtención de los datos personales. • Resultado de las auditorías o procedimientos de revisión efectuados.
Privilegiar los intereses y expectativa razonable de privacidad de los titulares. De acuerdo con el artículo 11, fracción II de los Lineamientos Generales, se entenderá que el CENAPRED privilegia los intereses del titular cuando el	2. Verificar los tratamientos que realiza el CENAPRED, a fin de confirmar que los mismos no den lugar a discriminación o trato injusto o arbitrario en contra del titular. 3. Elaborar avisos de privacidad con todos los elementos	Todas las unidades administrativas que realicen tratamiento de datos personales.	• Avisos de privacidad. • Documentación que se genere durante el tratamiento, que permita acreditar que los datos personales se utilizaron conforme a lo

Programa de Protección de Datos Personales

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
tratamiento de datos personales no da lugar a discriminación o trato injusto o arbitrario en contra del titular. Asimismo, de conformidad con el artículo 11, fracción III de los Lineamientos Generales, se entiende por expectativa razonable de privacidad, la confianza que el titular ha depositado en el CENAPRED respecto a que sus datos personales serán tratados conforme a lo señalado en el aviso de privacidad y en cumplimiento a las disposiciones previstas en la LGPDPPSO y los Lineamientos Generales. Esta obligación deberá observarse a lo largo de todo el ciclo de vida de los datos personales, desde la obtención de los mismos hasta su tratamiento y eliminación.	informativos que establece la LGPDPPSO, y con información que corresponda a la realidad del tratamiento que se efectúa. Ver obligación 3.O. 4. Incluir en los avisos de privacidad todas las finalidades de los tratamientos, las cuales deberán estar redactadas de forma clara y concreta, para que no haya lugar a confusión al respecto. Ver obligación 3.O. 5. Llevar a cabo el tratamiento de los datos personales sólo para los fines informados en el aviso de privacidad. Ver obligación 1.U.		señalado en el aviso de privacidad, y según lo dispuesto en la normatividad. • Resultado de las auditorías o procedimientos de revisión efectuados.

Artículos vinculados: 19 de la LGPDPPSO y 11 de los Lineamientos Generales.

Comprobación:	Sí	No
1. Se ha verificado que en todos los tratamientos que realiza el CENAPRED no se obtienen los datos personales con dolo, mala fe o negligencia.	☐	☐
2. Los avisos de privacidad cuentan con todos los elementos informativos que establece la LGPDPPSO.	☐	☐
3. En los avisos de privacidad se incluyen todas las finalidades del tratamiento.	☐	☐
4. Los datos personales sólo se utilizan para las finalidades previstas en el aviso de privacidad.	☐	☐
5. Se ha verificado que todos los tratamientos que realiza el CENAPRED no dan lugar a discriminación o	☐	☐

trato injusto o arbitrario en contra del titular.		

3.O. INFORMACIÓN (AVISO DE PRIVACIDAD)

Ver Criterios para la elaboración de avisos de privacidad en el Centro Nacional de Prevención de Desastres

4.O. MEDIDAS COMPENSATORIAS

Obligaciones	**Actividades para su cumplimiento**	**Unidad administrativa responsable del cumplimiento**	**Medios que facilitan la acreditación del cumplimiento**
Instrumentar medidas compensatorias cuando resulte imposible dar a conocer al titular el aviso de privacidad simplificado de manera directa, o ello exija esfuerzos desproporcionados, de acuerdo con los Criterios Generales para la instrumentación de medidas compensatorias en el sector público del orden federal, estatal y municipal. Las medidas compensatorias son mecanismos alternos para dar a conocer a los titulares el aviso de privacidad simplificado, a través de su difusión por medios masivos de comunicación u otros mecanismos de amplio alcance, como los siguientes: o Diario Oficial de la Federación o diarios de circulación nacional; o Diarios o gacetas oficiales de las entidades federativas, o diarios de circulación regional o local, o bien, revistas especializadas; o Página de Internet o cualquier otra plataforma o	1. Dar a conocer el aviso de privacidad simplificado a través de la implementación de medidas compensatorias cuando i) resulte imposible dar a conocer al titular el aviso de privacidad de manera directa, o ii) ello exija esfuerzos desproporcionados. 2. Evaluar si se requiere o no la autorización expresa del INAI para la implementación de medidas compensatorias, según lo dispuesto por los Criterios Generales para la instrumentación de medidas compensatorias en el sector público del orden federal, estatal y municipal. 3. Implementar las medidas compensatorias de conformidad con lo dispuesto por los Criterios Generales para la	Todas las unidades administrativas que realicen tratamiento de datos personales.	• Evidencia de la difusión del aviso de privacidad por el medio de comunicación masiva utilizado para la medida compensatoria implementada. • En su caso, autorización del INAI y evidencia de su difusión.

Programa de Protección de Datos Personales

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
tecnología oficial del responsable; o Carteles informativos; o Cápsulas informativas radiofónicas, o o Cualquier otro medio alterno de comunicación masivo. De conformidad con el artículo 2 de los Criterios Generales para la instrumentación de medidas compensatorias en el sector público del orden federal, estatal y municipal, se entiende por imposibilidad, esfuerzos desproporcionados y obtención directa, lo siguiente: **Imposibilidad de dar a conocer al titular el aviso de privacidad de forma directa:** se presenta cuando el responsable no cuenta con los datos personales necesarios que le permitan tener un contacto directo con el titular, ya sea porque no existen en sus archivos, registros, expedientes, bases o sistemas de datos personales, o bien, porque los mismos se encuentran desactualizados, incorrectos, incompletos o inexactos. **Esfuerzos desproporcionados para dar a conocer al titular el aviso de privacidad de forma directa:** cuando el número de titulares sea tal, que el hecho de poner a disposición de cada uno de éstos el aviso de privacidad, de manera directa, le implique al responsable un costo excesivo atendiendo a su suficiencia presupuestaria, o	instrumentación de medidas compensatorias en el sector público del orden federal, estatal y municipal.		

Programa de Protección de Datos Personales

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
comprometa la viabilidad de su presupuesto programado o la realización de sus funciones o atribuciones que la normatividad aplicable le confiera; o altere de manera significativa aquellas actividades que lleva a cabo cotidianamente en el ejercicio de sus funciones o atribuciones. **Obtención directa de los datos personales**: cuando el titular proporciona personalmente sus datos personales a quien representa al responsable o a través de algún medio que permita su entrega directa como podrían ser sistemas o medios electrónicos, ópticos, sonoros, visuales, vía telefónica, Internet o cualquier otra tecnología o medio físico.			

Artículos vinculados: 26 de la LGPDPPSO y Criterios Generales para la instrumentación de medidas compensatorias en el sector público del orden federal, estatal y municipal.

Comprobación:	Sí	No
1. Se tienen identificados los casos en los que se requiere la implementación de medidas compensatorias.	☐	☐
2. Se han implementado las medidas compensatorias en esos casos.	☐	☐
3. Se ha revisado que en dichos casos haya sido imposible dar a conocer el aviso de privacidad de manera directa al titular o ello exija esfuerzos desproporcionados.	☐	☐
4. Se ha evaluado si se requiere o no la autorización expresa del INAI.	☐	☐
5. Se ha revisado que se cumple con los requisitos de los Criterios Generales para la instrumentación de medidas compensatorias en el sector público del orden federal, estatal y municipal.	☐	☐

Programa de Protección de Datos Personales

5.O. CONSENTIMIENTO

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
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 de la LGPDPPSO, que señala lo siguiente: ***Artículo 22.*** *El responsable no estará obligado a recabar el consentimiento del titular para el tratamiento de sus datos personales en los siguientes casos:* ***I.*** *Cuando una ley así lo disponga, debiendo dichos supuestos ser acordes con las bases, principios y disposiciones establecidos en esta Ley, en ningún caso, podrán contravenirla;* ***II.*** *Cuando las transferencias que se realicen entre responsables, sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;* ***III.*** *Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;* ***IV.*** *Para el reconocimiento o defensa de derechos del titular ante autoridad competente;* ***V.*** *Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;* ***VI.*** *Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;* ***VII.*** *Cuando los datos personales sean*	1. Identificar las finalidades para las cuales se requiere el consentimiento de los titulares. 2. En esos casos, solicitar el consentimiento de los titulares según las reglas que se definen a continuación.	Todas las unidades administrativas que realicen tratamiento de datos personales.	Consentimiento expreso otorgado por los titulares y la solicitud respectiva. Aviso de privacidad y procedimiento para su puesta a disposición.

Programa de Protección de Datos Personales

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
necesarios para efectuar un tratamiento para la prevención, diagnóstico, la prestación de asistencia sanitaria; ***VIII.*** *Cuando los datos personales figuren en fuentes de acceso público;* ***IX.*** *Cuando los datos personales se sometan a un procedimiento previo de disociación, o* ***X.*** *Cuando el titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley en la materia.* La actualización de alguno de los supuestos anteriores no exime al responsable del cumplimiento de las demás obligaciones establecidas en la LGPDPPSO y los Lineamientos Generales.			
El consentimiento que, en su caso, se obtenga debe ser **libre, específico e informado**, según lo dispuesto por el artículo 20 de la LGPDPPSO: ***Artículo 20.*** *Cuando no se actualicen algunas de las causales de excepción previstas en el artículo 22 de la presente Ley, el responsable deberá contar con el consentimiento previo del titular para el tratamiento de los datos personales, el cual deberá otorgarse de forma:* ***I.*** *Libre: Sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular;* ***II.*** *Específica: Referida a finalidades concretas, lícitas, explícitas y legítimas que justifiquen el tratamiento, e* ***III.*** *Informada: Que el titular tenga conocimiento del aviso de privacidad previo al tratamiento a que serán sometidos sus datos personales.*	3. Solicitar el consentimiento después de que se ponga a disposición del titular el aviso de privacidad. 4. Redactar las solicitudes de consentimiento de forma tal que éste sea libre, específico e informado, y que las solicitudes sean concisas e inteligibles, estén en un lenguaje claro y sencillo acorde con el perfil del titular, y se distingan de asuntos ajenos a la protección de datos personales, cuando ello sea necesario.	Todas las unidades administrativas que realicen tratamiento de datos personales.	Procedimiento implementado para la solicitud del consentimiento. Procedimiento para la puesta a disposición del aviso de privacidad. Texto de solicitud de consentimiento.

Programa de Protección de Datos Personales

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
Por otra parte, la solicitud del consentimiento deberá ser concisa e inteligible, estar redactada en un lenguaje claro y sencillo acorde con el perfil del titular y, cuando se refiera a diversos asuntos ajenos a la protección de datos personales, deberá presentarse de tal forma que se distinga claramente de dichos asuntos.			
Dependiendo del tipo de datos personales, el consentimiento deberá ser tácito o expreso, siguiendo las reglas establecidas en el artículo 21 de la LGPDPPP: Cuando los datos sean sensibles y no se actualice alguna de las causales del artículo 22 de la LGPDPPSO, se requerirá el consentimiento **expreso y por escrito**, es decir, a través de la firma autógrafa o firma electrónica del titular, o por medio del mecanismo de autenticación que para tal efecto se establezca. El consentimiento **expreso** se solicitará cuando así lo exija una ley o las disposiciones aplicables. En todos los demás casos se podrá obtener el consentimiento **tácito**. El consentimiento será tácito cuando habiéndose puesto a disposición del titular el aviso de privacidad, éste no manifieste su voluntad en contrario. El consentimiento será expreso cuando la voluntad del titular se manifieste de forma verbal, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier	5. Definir el tipo de consentimiento que se requiere, según las categorías de datos personales que se vayan a tratar o las disposiciones normativas que regulen el tratamiento. 6. Habilitar los mecanismos necesarios para solicitar el consentimiento expreso, en los términos señalados en la columna anterior, así como documentar su obtención. 7. Documentar la puesta a disposición del aviso de privacidad para la obtención del consentimiento tácito.	Todas las unidades administrativas que realicen tratamiento de datos personales.	• Solicitud del consentimiento expreso. • Consentimiento expreso otorgado por los titulares. • Puesta a disposición del aviso de privacidad.

Programa de Protección de Datos Personales

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
otra tecnología. Para la obtención del consentimiento expreso, el responsable deberá facilitar al titular un medio sencillo y gratuito a través del cual pueda manifestar su voluntad, el cual le permita acreditar de manera indubitable y, en su caso, documentar que el titular otorgó su consentimiento ya sea a través de una declaración o una acción afirmativa clara. El silencio, las casillas previamente marcadas, la inacción del titular o cualquier otra conducta o mecanismo similar a los mencionados no deberán considerarse como consentimiento expreso del titular. Se entenderá que: El titular otorga su consentimiento de manera verbal cuando lo externe oralmente de manera presencial o mediante el uso de cualquier otra tecnología que permita la interlocución oral, en ambos casos, ante la persona que represente al responsable, y El titular otorga su consentimiento por escrito cuando manifieste su voluntad en un documento, físico o electrónico, a través de cierta declaración en sentido afirmativo, firma autógrafa, huella dactilar, firma electrónica o cualquier mecanismo o procedimiento equivalente autorizado por la normatividad aplicable. La carga de la prueba para acreditar la obtención del consentimiento expreso			

Programa de Protección de Datos Personales

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
correrá a cargo del responsable.			
Cuando los datos personales se recaben **directamente** del titular, y se requiera al consentimiento, éste deberá solicitarse previo a la obtención de los datos personales y después de la puesta a disposición del aviso de privacidad. Se entenderá que el responsable obtiene los datos personales directamente del titular cuando es éste quien los proporciona o la persona que lo representa, personalmente o por algún medio que permita su entrega directa como podrían ser medios electrónicos, ópticos, sonoros, visuales, vía telefónica, Internet o cualquier otra tecnología y/o medio.	8. Solicitar el consentimiento previo a la obtención de los datos personales y después de la puesta a disposición del aviso de privacidad, cuando los datos personales se obtengan directamente de su titular o representante.	Todas las unidades administrativas del CENAPRED que realicen tratamiento de datos personales.	• Procedimiento para la solicitud del consentimiento. • Aviso de privacidad y procedimiento para su puesta a disposición. • Consentimiento expreso otorgado.
Cuando los datos personales se obtengan **indirectamente** del titular, y se requiera el consentimiento, no se podrán tratar los datos personales hasta que se cuente con la manifestación libre, específica e informada del titular, en la que autorice el tratamiento de sus datos personales de manera tácita o expresa, según corresponda. De conformidad con el segundo y tercer párrafo del artículo 15 de los Lineamientos Generales, el titular tendrá un plazo de cinco días, contados a partir del día siguiente de recibir el aviso de privacidad por parte del responsable, para que, en su caso, manifieste su negativa al tratamiento de sus datos personales a través de los medios establecidos por el responsable. En caso de que el titular no manifieste	9. Cuando los datos personales no los proporcione personal o directamente el titular o su representante, el CENAPRED deberá enviar a los titulares el aviso de privacidad correspondiente al medio de contacto que tenga registrado. Asimismo, deberá informarles que cuentan con un plazo de 5 días hábiles para en su caso manifestar su negativa para el tratamiento de sus datos personales para aquellas finalidades que requieran su consentimiento. Si el titular no manifiesta su negativa en el plazo de cinco días antes señalado, el CENAPRED podrá	Todas las unidades administrativas del CENAPRED que realicen tratamiento de datos personales.	• Aviso de privacidad. • Constancia de envío del aviso de privacidad. Se sugiere utilizar un medio que permita acreditar la fecha en la que el titular recibió el aviso de privacidad. • Respuesta por parte de los titulares. • Consentimiento expreso otorgado.

Programa de Protección de Datos Personales

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
su negativa en el plazo antes señalado, se entenderá que ha otorgado su consentimiento tácito para el tratamiento de sus datos personales, salvo prueba en contrario. Se entenderá que se obtienen los datos personales de manera indirecta cuando no se cumplan con las condiciones señaladas en el apartado anterior.	suponer que cuenta con el consentimiento tácito. En el caso del consentimiento expreso, es necesario que el mismo se solicite, ya sea en el cuerpo del aviso de privacidad o en un instrumento aparte. El CENAPRED no podrá tratar los datos personales si no cuenta con el consentimiento expreso del titular.		
Atender las solicitudes de revocación del consentimiento, mismas que podrán ser presentadas por el titular en cualquier momento del tratamiento sin que se le atribuyan efectos retroactivos, a través del ejercicio de los derechos de oposición y cancelación.	10 Prever en el procedimiento interno para la atención de solicitudes de derechos ARCO lo relativo a la revocación del consentimiento, según los plazos, requisitos y procedimiento que se establecen para el ejercicio de los derechos de cancelación y oposición.	Comité de Transparencia y Unidad de Transparencia del CENAPRED.	• Procedimiento interno atención derechos ARCO.

Artículos vinculados: 20, 21 y 22 de la LGPDPPSO y 12 al 20 de los Lineamientos Generales.

Comprobación:	**Sí**	**No**
1. Se han identificado las finalidades para las cuales se requiere el consentimiento.	☐	☐
2. Se ha definido el tipo de consentimiento que se requiere, según el tipo de datos personales que se tratan y tomando en cuenta las disposiciones normativas que regulan el tratamiento.	☐	☐
3. Se han habilitado los mecanismos para solicitar el consentimiento expreso, en su caso.	☐	☐
4. El consentimiento se requiere después de que se da a conocer el aviso de privacidad.	☐	☐
5. Se encuentra documentada la puesta a disposición del aviso de privacidad y la obtención del consentimiento expreso, en su caso.	☐	☐
6. Las solicitudes de consentimiento se encuentran redactadas de forma tal que éste sea libre, específico e informado, y de que las solicitudes sean concisas e inteligibles, estén en un lenguaje claro y sencillo	☐	☐

acorde con el perfil del titular, y se distingan de asuntos ajenos a la protección de datos personales, cuando ello sea necesario.		
7. Cuando los datos personales se recaban directamente del titular, el consentimiento se solicita previo a la obtención de los datos personales y después de la puesta a disposición del aviso de privacidad.	☐	☐
8. Cuando los datos personales se recaban de manera indirecta, (i) se envía el aviso de privacidad correspondiente a los titulares; (ii) se les informa sobre los 5 días hábiles que tienen para manifestar su negativa; (iii) en caso de que se requiera el consentimiento expreso, éste se solicita y los datos personales se tratan sólo si se cuenta con el mismo.	☐	☐
9. El procedimiento interno para atención de derechos ARCO contempla lo relativo a la revocación del consentimiento.	☐	☐

6.O. CONSENTIMIENTO MENORES DE EDAD Y PERSONAS EN ESTADO DE INTERDICCIÓN O INCAPACIDAD DECLARADA CONFORME A LA LEY.

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
Atender las reglas de representación previstas en el Código Civil Federal y demás disposiciones que resulten aplicables en la materia específica de que se trate, para la obtención del consentimiento de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad declarada conforme a la ley. Asimismo, tomar como referencia lo dispuesto en los artículos 78 a 81 de los Lineamientos Generales para acreditar la identidad de los menores de edad menores de edad o de personas que se encuentren en estado de interdicción o incapacidad declarada conforme a la ley.	1. Identificar los tratamientos de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad declarada conforme a la ley, que requieren consentimiento, según el artículo 22 de la LGPDPPSO. 2. Poner a disposición de los padres, tutores o representantes legales el aviso de privacidad, así como también, cuando ello sea posible, a los menores de edad y al titular en estado de interdicción o incapacidad declarada conforme a ley. 3. Redactar los avisos de privacidad y solicitudes de consentimiento en lenguaje sencillo, adaptado para la comprensión del menor de edad o de la persona que se encuentre en	Todas las unidades administrativas del CENAPRED que realicen tratamiento de datos personales.	• Documentación que acompañe la solicitud y el otorgamiento del consentimiento por parte de los padres, tutores o representantes legales.

	estado de interdicción o incapacidad declarada conforme a ley. 4. Implementar mecanismos que permitan tener certeza que quien otorga el consentimiento, está facultado legalmente para ello, máxime cuando el mismo no se vaya a requerir con la presencia física de los padres, tutores o representantes legales. Se sugiere consultar estos mecanismos previamente con el Comité de Transparencia y/o el Oficial de Privacidad.		

Artículos vinculados: 20 de la LGPDPPSO y 78 a 81 de los Lineamientos Generales.

Comprobación:	**Sí**	**No**
1. Se tienen identificados los tratamientos de menores de edad y personas que se encuentren en estado de interdicción o incapacidad declarada conforme a la ley, que requieren consentimiento.	☐	☐
2. El aviso de privacidad se pone a disposición de los padres, tutores o representantes legales el aviso de privacidad, así como también, cuando ello es posible, del menor de edad o de la persona que se encuentre en estado de interdicción o incapacidad declarada conforme a ley.	☐	☐
3. Los avisos de privacidad y solicitudes de consentimiento se redactaron en un lenguaje sencillo, para su comprensión por parte de los menores de edad y personas que se encuentren en estado de interdicción o incapacidad declarada conforme a la ley.	☐	☐
4. Se solicita el consentimiento a la persona habilitada para ello según las reglas de representación del Código Civil Federal.	☐	☐
5. Se han implementado mecanismos para tener certeza de que el consentimiento lo otorga la persona habilitada para tal fin (padres, tutores o representantes legales).	☐	☐
6. La identidad de los menores y sus representantes se acredita conforme a lo dispuesto por los artículos 76 a 81 de los Lineamientos Generales.	☐	☐

7.O. DATOS PERSONALES SENSIBLES

Programa de Protección de Datos Personales

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del tratamiento	Medios para acreditar el cumplimiento
No 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.	1. Revisar la necesidad y legalidad del tratamiento de datos personales sensibles para cumplir con la finalidad de que se trate, a fin de que quede debidamente justificada su obtención y uso. 2. Revisar que se actualice alguno de los supuestos del artículo 22 de la LGPDPPSO, o bien, en caso contrario, solicitar el consentimiento expreso y por escrito del titular.	Todas las unidades administrativas del CENAPRED que realicen tratamiento de datos personales.	• Marco normativo que habilita para el tratamiento de datos personales sensibles. • Consentimiento del titular, en su caso, o la actualización de alguno de los supuestos previstos en el artículo 22 de la LGPDPPSO.
No llevar a cabo tratamiento de datos personales que tengan como efecto la discriminación de los titulares por su origen étnico o racial, su estado de salud presente, pasado o futuro, su información genética, sus opiniones políticas, su religión o creencias filosóficas o morales y su preferencia sexual.	3. Verificar que el tratamiento de datos personales no tenga como consecuencia discriminación de los titulares.	Todas las unidades administrativas del CENAPRED que realicen tratamiento de datos personales.	• Documentación que se genere en torno al tratamiento.

Artículos vinculados: 7 de la LGPDPPSO y 53 de los Lineamientos Generales.

Comprobación:	Sí	No
1. El tratamiento de datos personales sensibles está debidamente justificado por las atribuciones de la unidad administrativa y el principio de necesidad.	☐	☐
2. Se tienen identificados los casos en los que se requiere el consentimiento expreso y por escrito de los titulares.	☐	☐
3. Se obtiene el consentimiento expreso y por escrito del titular.	☐	☐
4. Se ha verificado que el tratamiento no tenga como consecuencia discriminación para los titulares.	☐	☐

8.O. INTERÉS SUPERIOR DE LOS MENORES DE EDAD

Obligaciones	Actividades para su	Unidad administrativa	Medios para acreditar el

Programa de Protección de Datos Personales

	cumplimiento	**responsable del cumplimiento**	**cumplimiento**
Privilegiar el interés superior del niño, niña y adolescente en el tratamiento de sus datos personales, en términos de las disposiciones previstas en la Ley General de los Derechos de Niñas, Niños y Adolescentes, así como lo dispuesto en la Ley General y los Lineamientos Generales. Esta obligación se deberá observar en todo el ciclo de vida de los datos personales, desde la obtención de los datos personales de menores de edad, hasta su tratamiento y cancelación.	1. En todos los casos en que estén involucrados datos personales de menores de edad, tener siempre en cuenta y privilegiar el interés superior del menor de edad. 2. Conocer la Ley General de Niñas, Niños y Adolescentes, con objeto de conocer los derechos de los menores de edad y las obligaciones al respecto. 3. Poner a disposición el aviso de privacidad tanto al adulto que tenga la representación del menor, como al propio titular de los datos personales. 4. Solicitar el consentimiento del adulto que tenga la representación del menor, cuando éste se requiera, y de manera adicional solicitar la opinión del propio titular.	Todas las unidades administrativas del CENAPRED que realicen tratamiento de datos personales.	• Documentación o procedimiento que acredite la puesta a disposición del aviso de privacidad al adulto que tenga la representación del menor de edad y al propio titular de los datos personales. • Documento que acredite la obtención del consentimiento del adulto que tiene la representación del menor, así como la opinión del propio titular. • Capacitación o curso realizado en materia de la Ley General de Niñas, Niños y Adolescentes, o bien, difusión de la misma.

Artículos vinculados: 7 de la LGPDPPSO y 5 de los Lineamientos Generales.

Comprobación:	**Sí**	**No**
1. Se privilegia el interés superior del menor en el tratamiento de datos personales.	☐	☐
2. Se conoce la Ley General de Niñas, Niños y Adolescentes.	☐	☐
3. Se obtuvo el consentimiento del adulto en representación del menor, y se solicitó la opinión del menor, en su caso.	☐	☐

9.O. PROPORCIONALIDAD

Programa de Protección de Datos Personales

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
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, de acuerdo con las atribuciones conferidas al responsable por la normatividad que le resulte aplicable	1. Identificar qué datos personales se requieren para cada una de las finalidades. El listado de datos personales debe estar completo con independencia de que en el aviso de privacidad se informe por categoría de datos. 2. Analizar y revisar que se soliciten sólo aquellos datos personales que resultan indispensables para cumplir con las finalidades de que se trate. 3. Cuando una normativa establezca con precisión los datos personales que deberán obtenerse para cumplir con la finalidad de que se trate, sólo deberán solicitarse dichos datos.	Todas las unidades administrativas del CENAPRED que realicen tratamiento de datos personales.	• Avisos de privacidad. • Documentos, expedientes, archivos o bases de datos correspondientes al tratamiento. • Normatividad que establezca, en su caso, los datos personales que deberán solicitarse para el tratamiento específico.
Realizar esfuerzos razonables para limitar los datos personales tratados, al mínimo necesario, con relación a las finalidades que motivaron su tratamiento.	4. Requerir el mínimo posible de datos personales para lograr las finalidades para las cuales se tratan.	Todas las unidades administrativas del CENAPRED que realicen tratamiento de datos personales.	

Artículos vinculados: 25 de la LGPDPPSO y 24 y 25 de los Lineamientos Generales.

Comprobación:	**Sí**	**No**
1. Se tienen identificados los datos personales que se requieren para cada una de las finalidades.	☐	☐
2. Los datos personales que se solicitan son los mínimos necesarios para cumplir con las finalidades.	☐	☐

4.2.3. Obligaciones relevantes en la etapa de USO de los datos personales (U)

Programa de Protección de Datos Personales

1.U. FINALIDAD

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
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 del responsable, conforme a lo previsto en la legislación mexicana y el derecho internacional que le resulte aplicable, y **Legítimas:** cuando las finalidades que motivan el tratamiento de los datos personales se encuentran 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.	1. Identificar las finalidades de cada tratamiento que se realice, y verificar que las mismas atiendan a fines específicos o determinados, y que sean acordes a las atribuciones o facultades del CENAPRED y unidad administrativa de que se trate. 2. Verificar que en los avisos de privacidad se informan todas las finalidades para las cuales se tratan los datos personales, y que éstas se describen de manera clara. 3. Identificar qué finalidades requieren consentimiento y solicitarlo según las reglas descritas anteriormente.	Todas las unidades administrativas del CENAPRED que realicen tratamiento de datos personales.	• Avisos de privacidad. • Inventario de tratamientos de datos personales. • Documentos que se generen en el tratamiento.
Las finalidades deben estar relacionadas con las	4. Identificar el marco normativo (ley,	Todas las unidades administrativas del	• Marco normativo.

Programa de Protección de Datos Personales

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
atribuciones normativas de la unidad administrativa que realice el tratamiento.	reglamento, lineamiento, entre otros, con sus respectivos artículos) que otorga las atribuciones a la unidad administrativa para tratar los datos personales para cada una de las finalidades.	CENAPRED que realicen tratamiento de datos personales.	
Cuando se vayan a tratar los datos personales para finalidades distintas a las previstas en el aviso de privacidad, se requiere tener atribuciones legales para ello y el consentimiento del titular, salvo que se trate de una persona desaparecida. Se deberá considerar: **I.** La expectativa razonable de privacidad del titular, basada en la relación que tiene con éste; **II.** La naturaleza de los datos personales; **III.** Las consecuencias del tratamiento posterior de los datos personales para el titular, y **IV.** Las medidas adoptadas para que el tratamiento posterior de los datos personales cumpla con las disposiciones previstas en la Ley General y los presentes Lineamientos generales.	5. Identificar las finalidades que no fueron informadas en los avisos de privacidad y que se requieran llevar a cabo. 6. Verificar que existan atribuciones legales para el tratamiento de los datos personales para estas finalidades adicionales. 7. Solicitar el consentimiento de los titulares para el tratamiento de datos personales para estas finalidades adicionales, cuando el mismo se requiera. 8. Implementar las medidas que se requieran para cumplir con las obligaciones que establece la LGPDPPSO y los Lineamientos Generales, con relación a las finalidades adicionales.	Todas las unidades administrativas del CENAPRED que realicen tratamiento de datos personales.	• Marco normativo. • Consentimiento otorgado por los titulares o supuesto que se actualiza del artículo 22 de la LGPDPPSO.

Artículos vinculados: 18 de la LGPDPPSO y 9 y 10 de los Lineamientos Generales.

Comprobación:	**Sí**	**No**

Programa de Protección de Datos Personales

Se tienen identificadas cada una de las finalidades de cada tratamiento que realiza la unidad administrativa.	☐	☐
Estas finalidades atiendan a fines específicos o determinados, y que sean acordes a las atribuciones o facultades del CENAPRED y unidad administrativa de que se trate.	☐	☐
Estas finalidades son informadas en los avisos de privacidad de manera clara y completa.	☐	☐
Se ha identificado qué finalidades requieren el consentimiento y el mismo se ha solicitado.	☐	☐
Las finalidades están vinculadas a las atribuciones de la unidad administrativa, de forma tal que son lícitas y legítimas.	☐	☐
Se tienen identificadas las finalidades que no fueron informadas en su momento en los avisos de privacidad, pero que se requieren llevar a cabo.	☐	☐
Se ha verificado que hay atribuciones legales para llevar a cabo estas finalidades adicionales.	☐	☐
Se ha solicitado el consentimiento de los titulares para las finalidades adicionales, en caso de requerirse, o se ha identificado que se actualiza alguno de los supuestos previstos en el artículo 22 de la LGPDPPSO.	☐	☐
Se han definidor e implementado las medidas que se requieran para cumplir con las obligaciones que establece la LGPDPPSO y los Lineamientos Generales, con relación a las finalidades adicionales.	☐	☐

2.U. CALIDAD

Obligaciones	**Actividades para su cumplimiento**	**Unidad administrativa responsable del cumplimiento**	**Medios para acreditar el cumplimiento**
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, y	1. Implementar medidas para que los datos personales se actualicen y, en su caso, corrijan o completen, en las distintas bases de datos que estén a cargo de la unidad administrativa. Estas medidas deberán permitir que la modificación de los datos personales sea inmediata, una vez que la unidad administrativa tenga conocimiento de la	Todas las unidades administrativas del CENAPRED que realicen tratamiento de datos personales.	• Base de datos actualizada y correcta. • Constancias o anotaciones sobre la rectificación realizada, en aquellos casos en que la misma haya sido procedente.

Programa de Protección de Datos Personales

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
Actualizados: cuando los datos personales responden fielmente a la situación actual del titular.	actualización o corrección a que haya lugar.		
Establecer plazos de conservación de los datos personales, los cuales no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron su tratamiento, asimismo deberán atender las disposiciones aplicables en la materia de que se trate y considerar los aspectos administrativos, contables, fiscales, jurídicos e históricos de los datos personales.	2. Establecer los plazos de conservación de los datos personales, para cada uno de los tratamientos, lo cual deberá ser congruente con los plazos de conservación establecidos en los instrumentos de clasificación archivística.	Todas las unidades administrativas del CENAPRED que realicen tratamiento de datos personales con el apoyo de la persona designada como responsable del archivo de trámite del CENAPRED	• Instrumentos de clasificación archivística.
Establecer y documentar los procedimientos para la conservación y supresión de los datos personales, en los cuales se incluyan los periodos de conservación, mecanismos que permitan cumplir con dichos plazos, así como realizar una revisión periódica sobre la necesidad de conservar los datos personales.	3. Elaborar los procedimientos para la conservación y supresión de los datos personales, así como documentarlos. Estos procedimientos podrán ser los establecidos en materia de archivos, si a través de los mismos se puede cumplir con la obligación prevista en la LGPDPPSO.	La persona designada como responsable del archivo de trámite del CENAPRED	• Procedimientos desarrollados. • Documentación y evidencia que se genere con su implementación.

Artículos vinculados: 23 y 24 de la LGPDPPSO y 21 y 22 de los Lineamientos Generales.

Comprobación:	**Sí**	**No**
Se cuenta con medidas para actualizar, corregir o completar los datos personales de cualquier base de datos que está a cargo de la unidad administrativa.	☐	☐

Programa de Protección de Datos Personales

Se tienen establecidos los plazos de conservación de los datos personales por cada tratamiento.	☐	☐
Los plazos de conservación son congruentes con los establecidos en los instrumentos de archivo.	☐	☐
Se cuenta con procedimientos para la conservación y supresión de los datos personales y éstos se encuentran documentados.	☐	☐

3.U. RELACIÓN CON LOS ENCARGADOS

Obligaciones	**Actividades para su cumplimiento**	**Unidad administrativa responsable del cumplimiento**	**Medios para acreditar el cumplimiento**
Formalizar las relaciones con los encargados mediante contrato o instrumento jurídico, que permita acreditar su existencia, alcance y contenido. Incluir en el contrato o instrumento jurídico, al menos, las siguientes obligaciones del encargado: Realizar el tratamiento de los datos personales conforme a las instrucciones del responsable; Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable; Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables; Informar al responsable cuando ocurra una vulneración a los datos personales que trata por sus instrucciones; Guardar confidencialidad respecto de los datos personales tratados; Suprimir o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales; Abstenerse de transferir los datos personales salvo en el caso de que el	1. Formalizar las relaciones con los encargados mediante contrato o instrumento jurídico, que contenga las obligaciones y cláusulas antes señaladas.	La Coordinación Administrativa, la Dirección de Servicios Técnicos a través de la Subdirección Jurídica y unidades administrativas requirentes.	• Cláusula tipo • Contratos o instrumentos jurídicos.

Programa de Protección de Datos Personales

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
responsable así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente; Permitir al INAI o al responsable, realizar verificaciones en el lugar o establecimiento donde se lleva a cabo el tratamiento de los datos personales; Colaborar con el INAI en las investigaciones previas y verificaciones que lleve a cabo en términos de lo dispuesto en la LGPDPPSO y los Lineamientos Generales, proporcionando la información y documentación que se estime necesaria para tal efecto, así como Generar, actualizar y conservar la documentación necesaria que le permita acreditar el cumplimiento de sus obligaciones.			
Autorizar las subcontrataciones que realicen los encargados y que involucren el tratamiento de datos personales. Informar al encargado que el contrato o el instrumento jurídico mediante el cual se formalice la subcontratación deberá incluir cláusulas con las obligaciones antes señaladas.	2. Incluir en los contratos originales con los encargados una cláusula que haga referencia a lo que procederá en caso de que el encargado desee subcontratar servicios que involucren el tratamiento de datos personales. En el contrato original se podrá autorizar o prohibir de manera directa la subcontratación de este tipo de servicios, o bien, se podrá establecer que para la subcontratación será necesario que el encargado solicite autorización expresa al responsable, caso por caso. Las autorizaciones se	La Coordinación Administrativa, la Dirección de Servicios Técnicos a través de la Subdirección Jurídica y unidades administrativas requirentes	• Cláusula tipo • Contratos o instrumentos jurídicos.

Programa de Protección de Datos Personales

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
	podrán otorgar desde el contrato original, cuando el encargado ya prevea subcontrataciones específicas, y garantice que las mismas se realizarán en las condiciones antes señaladas. En caso contrario, la autorización se realizará de manera posterior. Para el cumplimiento de esta obligación, es necesario que el contrato o el instrumento jurídico, celebrado de origen con el encargado, establezca que las subcontrataciones que no se establezcan de manera expresa en dicho contrato o instrumento deberán ser autorizadas por el responsable. Asimismo, si se van a autorizar las subcontrataciones o quedará abierta dicha posibilidad, será necesario que en el contrato original entre el responsable y el encargado, se establezca que si este último pretende llevar a cabo subcontrataciones deberá suscribir un contrato o instrumento jurídico con el tercero de que se trate, en el que se deberán prever las cláusulas a las que refiere la columna anterior como parte de las obligaciones del subcontratado.		

Programa de Protección de Datos Personales

Artículos vinculados: 59 y 61 de la LGPDPPSO y 108 a 110 de los Lineamientos Generales.

Comprobación:	**Sí**	**No**
Las relaciones con los encargados se formalizan mediante contratos o instrumentos jurídicos.	☐	☐
Estos contratos o instrumentos jurídicos establecen cláusulas con las siguientes obligaciones del encargado: Realizar el tratamiento de los datos personales conforme a las instrucciones del responsable; Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable; Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables; Informar al responsable cuando ocurra una vulneración a los datos personales que trata por sus instrucciones; Guardar confidencialidad respecto de los datos personales tratados; Suprimir o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales; Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente; Permitir al INAI o al responsable realizar verificaciones en el lugar o establecimiento donde lleva a cabo el tratamiento de los datos personales; Colaborar con el INAI en las investigaciones previas y verificaciones que lleve a cabo en términos de lo dispuesto en la LGPDPPSO y los Lineamientos Generales, proporcionando la información y documentación que se estime necesaria para tal efecto, y Generar, actualizar y conservar la documentación necesaria que le permita acreditar el cumplimiento de sus obligaciones.	☐	☐
El contrato original establece una cláusula mediante la cual se autoriza subcontrataciones y/o que establezca que todas las subcontrataciones deberán ser autorizadas por el responsable.	☐	☐
Las subcontrataciones que se autorizan son específicas y se encuentran contenidas en un contrato o instrumento jurídico que establezca las cláusulas aplicables al encargado.	☐	☐
Se informa al encargado la obligación de incluir en el contrato o instrumento jurídico mediante el cual se formalice la subcontratación, las obligaciones antes señaladas para el tercero subcontratado.	☐	☐

5.U. TRANSFERENCIAS

Obligaciones	**Actividades para su cumplimiento**	**Unidad administrativa responsable del cumplimiento**	**Medios para acreditar el cumplimiento**
Formalizar las transferencias	1. Identificar las	Todas las unidades	• Cláusulas

Programa de Protección de Datos Personales

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
nacionales e internacionales mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes, salvo en las siguientes excepciones: Cuando la transferencia sea nacional y se realice entre el CENAPRED y otros responsables en virtud del cumplimiento de una disposición legal o en el ejercicio de atribuciones expresamente conferidas a éstos, o Cuando la transferencia sea internacional y se encuentre prevista en una ley o tratado suscrito y ratificado por México, o bien, se realice a petición de una autoridad extranjera u organismo internacional competente en su carácter de receptor, siempre y cuando las facultades entre el CENAPRED y el responsable receptor sean homólogas, o bien, las finalidades que motivan la transferencia sean análogas o compatibles respecto de aquéllas que dieron origen al tratamiento que realiza el CENAPRED.	transferencias que se realizan que requieren la suscripción de cláusulas contractuales, convenios de colaboración u otro instrumento jurídico, que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes. 2. Elaborar y suscribir las cláusulas contractuales, convenios de colaboración u otro instrumento jurídico, cuando se requiera.	administrativas del CENAPRED que realicen transferencias. La Dirección de Servicios Técnicos, con el apoyo de las unidades administrativas, en lo relativo a la elaboración y suscripción de las cláusulas contractuales, convenios de colaboración u otros instrumentos jurídicos.	contractuales, convenios de colaboración u otros instrumentos jurídicos.
Sólo hacer transferencias fuera del territorio nacional cuando el tercero receptor se obligue a proteger los datos personales conforme a los principios y deberes que establece la LGPDPPSO y las disposiciones que resulten aplicables en la materia.	3. Para las transferencias y remisiones internacionales, previo a que éstas ocurran, se deberá solicitar al tercero receptor que manifieste por escrito que se obliga a proteger los datos personales conforme a los principios y deberes que establece la LGPDPPSO y las	Todas las unidades administrativas del CENAPRED que realicen transferencias.	• Escritos de los terceros receptores de los datos personales.

Programa de Protección de Datos Personales

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
	disposiciones que resulten aplicables en la materia.		
Comunicar el aviso de privacidad respectivo al tercero receptor en las transferencias nacionales e internacionales que se realicen.	4. Cuando inicien las transferencias, comunicar el aviso de privacidad correspondiente. En lo sucesivo, sólo comunicar las modificaciones al aviso de privacidad original, cuando existan.	Todas las unidades administrativas del CENAPRED que realicen transferencias.	• Evidencia de la comunicación del aviso de privacidad.
Solicitar el consentimiento para las transferencias nacionales e internacionales, salvo en los siguientes casos: Cuando la transferencia sea nacional y se realice entre el CENAPRED y otros responsables en virtud del cumplimiento de una disposición legal o en el ejercicio de atribuciones expresamente conferidas a éstos; Cuando la transferencia sea internacional y se encuentre prevista en una ley o tratado suscrito y ratificado por México; Cuando la transferencia internacional se realice a petición de una autoridad extranjera u organismo internacional competente en su carácter de receptor, siempre y cuando las facultades entre el CENAPRED y el responsable receptor sean homólogas, o bien, las finalidades que motivan la transferencia sean análogas o compatibles respecto de aquéllas que dieron origen al tratamiento que realiza el CENAPRED; Cuando la transferencia se realice entre responsables, siempre y cuando los datos personales se utilicen para el ejercicio de facultades propias,	5. Identificar las transferencias que requieren consentimiento de los titulares e informarlo en el aviso de privacidad. 6. Solicitar el consentimiento de los titulares previo a la transferencia, cuando éste sea necesario y según la modalidad que se requiera (tácito o expreso y por escrito).	Todas las unidades administrativas del CENAPRED que realicen transferencias.	• Consentimiento de los titulares.

Programa de Protección de Datos Personales

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales; Cuando la transferencia sea legalmente exigida para la investigación y persecución de los delitos, así como la procuración o administración de justicia; Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho ante autoridad competente, siempre y cuando medie el requerimiento de esta última; Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios, siempre y cuando dichos fines sean acreditados; Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el CENAPRED y el titular; Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el CENAPRED y un tercero; Cuando se trate de los casos en los que el CENAPRED no esté obligado a recabar el consentimiento del titular para el tratamiento y transmisión de sus datos personales, conforme a lo dispuesto en el artículo 22 de la LGPDPPSO; o Cuando la transferencia sea necesaria por razones de seguridad nacional.			
En caso de que se requiera el consentimiento expreso, establecer el medio que permita obtenerlo de manera previa a la transferencia. Este medio deberá ser de fácil acceso y con la mayor cobertura posible, y considerar el perfil de los titulares y la	7. Establecer los medios para solicitar el consentimiento expreso, previo a la transferencia.	Todas las unidades administrativas del CENAPRED que realicen transferencias.	• Medios establecidos para solicitar el consentimiento expreso, en caso de requerirse.

Programa de Protección de Datos Personales

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
forma en cómo se mantiene contacto cotidiano o común con ellos.			
Sólo tratar los datos que hayan sido transferidos al responsable para las finalidades para las cuales le hayan sido comunicados, según lo establecido en el aviso de privacidad proporcionado, así como garantizar la confidencialidad de los datos personales.	8. Implementar los controles de seguridad establecidos para la confidencialidad de los datos personales, y no tratar los datos personales para finalidades distintas.	Todas las unidades administrativas del CENAPRED que realicen transferencias.	• Controles implementados.

Artículos vinculados: 66, 67, 68, 69 y 70 de la LGPDPPSO y 113 a 118 de los Lineamientos Generales.

Comprobación:	Sí	No
Se tienen identificadas las transferencias que requieren la suscripción de cláusulas contractuales, convenios de colaboración u otro instrumento jurídico, que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes.	☐	☐
Se han elaborado y suscrito las cláusulas contractuales, convenios de colaboración u otro instrumento jurídico respectivos.	☐	☐
Se solicita al tercero receptor internacional que manifieste por escrito que se obliga a proteger los datos personales conforme a los principios y deberes que establece la LGPDPPSO y las disposiciones que resulten aplicables en la materia.	☐	☐
Se comunica al tercero receptor el aviso de privacidad correspondiente y, en su caso, sus modificaciones.	☐	☐
Se han identificado las transferencias que requieren el consentimiento y todas ellas son informadas en el aviso de privacidad.	☐	☐
Se solicita el consentimiento de los titulares, en su caso.	☐	☐
Se han establecido medios adecuados para solicitar el consentimiento expreso: que permitan obtenerlo de manera previa a la transferencia, que sean de fácil acceso y con la mayor cobertura posible, y que consideren el perfil de los titulares y la forma en cómo se mantiene contacto cotidiano o común con ellos.	☐	☐
Sólo se tratan los datos personales para las finalidades para las cuales fueron transferidos.	☐	☐
Se aplican controles de seguridad para la transferencia de los datos personales.	☐	☐

6.U. ATENCIÓN DE SOLICITUDES DE EJERCICIO DE DERECHOS ARCO

Programa de Protección de Datos Personales

Para el cumplimiento de obligaciones, actividades para su cumplimiento, unidades administrativas responsables y medios para acreditar su cumplimiento, observar lo establecido en la Política Interna de Protección de Datos Personales en el Centro Nacional de Prevención de DESASTRES y la Guía para ejercer los derechos de Acceso, Rectificación, Cancelación y Oposición de datos personales del Centro Nacional de Prevención de Desastres.

Comprobación:	**Sí**	**No**
El procedimiento interno, desarrollado por la Unidad de Transparencia, para recibir, turnar y responder las solicitudes de ejercicio de derechos ARCO prevé, al menos, lo siguiente: 1. La facilitación de la presentación de las solicitudes; 2. El turno y atención interna de manera eficiente, de conformidad con el procedimiento que establece la LGPDPPSO y los Lineamientos Generales, sin establecer mayores requisitos que los que señala la norma; 3. Que los servidores públicos estén informados sobre su obligación de orientar a los titulares a la Unidad de Transparencia cuando se requiera; 4. La obligación de entregar al solicitante un acuse; 5. La obligación de la Unidad de Transparencia de turnar las solicitudes a todas las unidades administrativas que pudieran tener los datos personales; 6. El registro en el sistema electrónico habilitado por el INAI de las solicitudes que se presenten por escrito libre; 7. Que las unidades administrativas turnen a la Unidad de Transparencia las solicitudes que reciben, al día siguiente de su presentación, aunque se tendrá por recibida en la fecha en que fue presentada en la unidad administrativa; 8. Plazos y acciones internas para que las solicitudes se respondan en los plazos de 20 y 15 días hábiles establecidos en la LGPDPPSO para responder las solicitudes y hacer efectivo el derecho, en su caso; 9. La justificación de la ampliación de plazo y la notificación al titular dentro del plazo de 20 días hábiles contados a partir del día siguiente; 10. La acreditación de la identidad del titular y, en su caso, la identidad y personalidad de su representante al momento de que se presente la solicitud o previo a hacer efectivo el derecho correspondiente; 11. La atención de las reglas de representación dispuestas en el Código Civil Federal y demás disposiciones jurídicas aplicables y lo señalado en el Anexo 8 de este Programa para el ejercicio de derechos ARCO de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad de conformidad con las leyes civiles; 12. La solicitud a quien pretenda ejercer derechos ARCO sobre datos personales de personas fallecidas, que acredite que el titular de los datos personales hubiere expresado fehacientemente su voluntad de que dicha persona pueda ejercer los derechos ARCO con relación a su información personal, o bien, confirmar que exista interés jurídico según lo dicho en este Programa; 13. La verificación de los pagos respectivos a los costos de reproducción y envío establecidos; 14. La verificación del cumplimiento de los requisitos que establece la LGPDPPSO y los Lineamientos Generales para la presentación de solicitudes de ejercicio de derechos ARCO;	☐	☐

Programa de Protección de Datos Personales

Comprobación:	Sí	No
15. La prevención, en su caso, en el plazo de 10 días contados a partir del día siguiente al de la notificación, y lo que implica en la atención de la solicitud; 16. La recepción de las pruebas que aporte el solicitante; 17. Dejar asentado en la constancia que acredite el ejercicio del derecho de que se trate, que el titular o su representante acreditaron su identidad y personalidad mediante la presentación de documentos originales, y describir estos últimos; 18. La atención de derechos ARCO de manera gratuita, realizando los cobros de reproducción y envío que prevé la norma; 19. El análisis sobre la procedencia de la excepción del pago de los costos de reproducción y envío cuando el titular haya manifestado que no puede cubrir los costos; 20. La atención de la modalidad de reproducción solicitada por el titular en las solicitudes del derecho de acceso, salvo que exista una imposibilidad física o jurídica, en cuyo caso se deberán ofrecer otras modalidades, y justificar y motivar esta acción; 21. El plazo de 3 días siguientes a la presentación de la solicitud si se va a declarar la incompetencia, y la orientación al CENAPRED competente si se conoce; 22. La declaración formal de inexistencia de los datos personales por parte del Comité de Transparencia, en su caso; 23. El plazo de 3 días siguientes a la presentación de la solicitud en caso de que se advierta que la solicitud para el ejercicio de derechos ARCO corresponda a un derecho diferente; 24. La inclusión de todos los elementos que se señalan en este Programa en la respuesta que se emita; 25. La notificación de las respuestas por los medios señalados en este Programa; 26. El acceso a los datos personales en el plazo de 15 días contados a partir del día siguiente a que se haya notificado la respuesta al titular, a través de los medios señalados en este Programa, una vez acreditada la identidad del titular o de su representante y la personalidad de este último; y verificado el pago de los costos de reproducción y envío correspondientes; 27. La generación de la constancia que acredite la rectificación de los datos personales con los datos que se señalan en este Programa, y su notificación al titular en el plazo de 15 días contados a partir del día siguiente a que se haya notificado la respuesta al titular, previa acreditación de su identidad y la de su representante y la personalidad de este último, en su caso; 28. La generación de la constancia de cancelación con la información señalada en este Programa en el plazo de 15 días contados a partir del día siguiente a que se haya notificado la respuesta al titular; y su notificación al titular en el plazo de 15 días contados a partir del día siguiente a que se haya notificado la respuesta al titular, previa acreditación de su identidad y la de su representante y la personalidad de este último, en su caso; 29. La generación de la constancia que notifique al titular o su representante, previa acreditación de identidad y personalidad, el cese en el tratamiento de datos personales en el plazo de 15 días contados a partir del día siguiente a que se haya notificado la respuesta al titular; 30. El mantenimiento del medio de reproducción con los datos solicitados y las constancias de ejercicio a disposición, por un plazo de 60 días, y la eliminación de éstos transcurrido dicho plazo sin que el titular o el responsable los hayan recogido; 31. El plazo de 5 días siguientes a la presentación de la solicitud para el ejercicio de los derechos		

Programa de Protección de Datos Personales

Comprobación:	**Sí**	**No**
ARCO para informar al titular cuando las disposiciones aplicables a determinados tratamientos de datos personales establezcan un trámite o procedimiento específico para solicitar el ejercicio de los derechos ARCO; 32. Medidas para que las personas con algún tipo de discapacidad o grupos vulnerables, puedan ejercer, en igualdad de circunstancias, su derecho a la protección de datos personales. 33. Informar al titular sobre la negativa para el ejercicio del derecho ARCO que corresponda en el plazo de 20 días hábiles constados a partir del día siguiente a la recepción de la solicitud.		
Se cuentan con medios y procedimientos para que los titulares presenten sus solicitudes de ejercicio de derechos ARCO, que sean de fácil acceso, con la mayor cobertura posible y que atiendan al perfil de los usuarios y la forma como se tiene contacto cotidiano o común con ellos.	☐	☐
Se han elaborado formularios, sistemas y otros métodos simplificados para facilitar a los titulares el ejercicio de los derechos ARCO, o se utilizan aquéllos que haya elaborado el INAI.	☐	☐
En estos formularios, sistemas y métodos simplificados se incluye un espacio para que el titular pueda manifestar la circunstancia de no poder cubrir los costos de reproducción y envío.	☐	☐
Se observan las causales bajo las cuales se podrá negar el ejercicio de los derechos ARCO, y se informa al titular sobre la negativa en el plazo de 20 días hábiles.	☐	☐
Se han establecido los acuerdos necesarios con instituciones públicas especializadas que pudieran auxiliar en la recepción, trámite y entrega de las respuestas a solicitudes de ejercicio de derechos ARCO, en la lengua indígena, braille o cualquier formato accesible correspondiente.	☐	☐

7.U. PORTABILIDAD

Obligaciones	**Actividades para su cumplimiento**	**Unidad administrativa responsable del cumplimiento**	**Medios para acreditar el cumplimiento**
Otorgar al titular una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos, cuando los mismos se traten en un formato con tales características, según los lineamientos que emita el SNT, en los cuales establezca los parámetros a considerar para determinar los supuestos en los que se estará en presencia de un formato estructurado y comúnmente utilizado, así	1. Atender las solicitudes del ejercicio del derecho de portabilidad según los criterios y parámetros establecidos por la LGPDPPSO y los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales, publicados en el Diario Oficial de la Federación el 12 de febrero de 2018.	Unidad de Transparencia y unidades administrativas responsables de atender las solicitudes de ejercicio de derechos ARCO.	• Documentación que se genere para atender las solicitudes de ejercicio del derecho de portabilidad.

como las normas técnicas, modalidades y procedimientos para la transferencia de datos personales.			

Para cumplir con esta obligación, es necesario tener en cuenta lo que señala el artículo 57 de la LGPDPPSO y 6 de los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales en relación con lo plasmado en la Política Interna de Protección de Datos Personales en el Centro Nacional de Prevención de Desastres, la Guía para ejercer los derechos de Acceso, Rectificación, Cancelación y Oposición de datos personales del Centro Nacional de Prevención de Desastres, así como en los Criterios para la elaboración de los Avisos de Privacidad del CENAPRED.

Artículos vinculados: 57 de la LGPDPPSO y en general los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales[2].

Comprobación:	**Sí**	**No**
Se atienden las solicitudes del ejercicio del derecho de portabilidad según los criterios y parámetros establecidos por la LGPDPPSO y los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales.	☐	☐

4.2.4. Obligaciones relevantes en la etapa de ELIMINACIÓN de los datos personales (E)

1.E. SUPRESIÓN DE LOS DATOS PERSONALES (CALIDAD)

Obligaciones	**Actividades para su cumplimiento**	**Unidad administrativa responsable del cumplimiento**	**Medios para acreditar el cumplimiento**
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.	1. Tener identificados los plazos de conservación de las series documentales que contienen datos personales. 2. Realizar la eliminación de los documentos correspondientes a dichas series documentales cuando haya concluido el plazo de conservación respectivo.	La persona servidora pública designada como encargada del archivo de trámite en el CENAPRED y en lo correspondiente la Coordinación Administrativa junto con la Dirección de Instrumentación y Cómputo, con conocimiento de las unidades administrativas.	• Instrumentos de clasificación archivística. • Evidencia generada en la eliminación de los documentos. • Inventario de datos personales

[2] Disponible en: http://dof.gob.mx/nota_detalle.php?codigo=5512847&fecha=12/02/2018

Programa de Protección de Datos Personales

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
Previo a la supresión procederá el bloqueo.	3. Considerar en el plazo de conservación y en el procedimiento de archivos, la etapa de bloqueo de los datos personales.	La persona servidora pública designada como encargada del archivo de trámite en el CENAPRED y en lo correspondiente la Coordinación Administrativa junto con la Dirección de Instrumentación y Cómputo, con conocimiento de las unidades administrativas.	• Procedimiento de archivo que incluye el bloqueo.
Establecer políticas, métodos y técnicas orientadas a la supresión definitiva de los datos personales, de tal manera que la probabilidad de recuperarlos o reutilizarlos sea mínima. En las políticas, métodos y técnicas, se deberá considerar, al menos, los siguientes atributos y el o los medios de almacenamiento, físicos y/o electrónicos en los que se encuentren los datos personales: **Irreversibilidad:** que el proceso utilizado no permita recuperar los datos personales; **Seguridad y confidencialidad:** que en la eliminación definitiva de los datos personales se consideren los deberes de confidencialidad y seguridad a que se refieren la LGPDPPSO y los Lineamientos Generales, y **Favorable al medio ambiente:** que el método utilizado produzca el mínimo de emisiones y desperdicios que afecten el medio ambiente.	4. Establecer las políticas, métodos y técnicas orientadas a la supresión definitiva de los datos personales, considerando los atributos de irreversibilidad; seguridad y confidencialidad y favorable al medio ambiente.	La persona servidora pública designada como encargada del archivo de trámite en el CENAPRED y en lo correspondiente la Coordinación Administrativa junto con la Dirección de Instrumentación y Cómputo, con conocimiento de las unidades administrativas.	• Políticas, métodos y técnicas desarrolladas. • Documentación y evidencia que se genere con su implementación.

Artículos vinculados: 23 de la LGPDPPSO y 23 de los Lineamientos Generales.

Programa de Protección de Datos Personales

Comprobación:	**Sí**	**No**
1. Se tienen identificados los plazos de conservación de las series documentales que contienen datos personales.	☐	☐
2. Se cuenta con un procedimiento para el bloqueo de los datos personales.	☐	☐
3. Se lleva a cabo la eliminación de los documentos correspondientes a las series documentales que contienen datos personales en el plazo establecido para ello.	☐	☐
4. Se cuenta con políticas, métodos y técnicas orientadas a la supresión definitiva de los datos personales, considerando los atributos de irreversibilidad; seguridad y confidencialidad y favorable al medio ambiente.	☐	☐

4.2.5. Otras obligaciones

RESPONSABILIDAD			
Obligaciones	**Actividades para su cumplimiento**	**Unidad administrativa responsable del cumplimiento**	**Medios para acreditar el cumplimiento**
Elaborar políticas y programas de protección de datos personales obligatorios y exigibles al interior de la organización, tomando en cuenta el desarrollo tecnológico y las técnicas existentes; la naturaleza, contexto, alcance, finalidades del tratamiento, atribuciones y facultades del responsable y demás cuestiones que se consideren convenientes. Para ello, el CENAPRED podrá valerse de estándares, mejores prácticas nacionales o internacionales, esquemas de mejores prácticas, o cualquier otro mecanismo que determine adecuado para tales fines.	2. Elaborar un programa de protección de datos personales que contemple el cumplimiento obligatorio al interior de la organización del responsable.	Comité de Transparencia.	• Programa 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.	3. Elaborar y aplicar un programa de capacitación y actualización de los servidores públicos en materia de protección de datos personales, de conformidad con el apartado de	Comité de Transparencia.	• Programa de capacitación para las personas servidoras públicas del CENAPRED.

Programa de Protección de Datos Personales

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
	Capacitación de este Programa.		
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 externas, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales. Las revisiones de las políticas y programas de seguridad y del sistema de supervisión y vigilancia implementados se deberá realizar cada dos años, salvo que se realicen modificaciones sustanciales a los tratamientos y sea necesaria una revisión previa.	4. Establecer un sistema de supervisión y vigilancia interna y/o externa para comprobar el cumplimiento de este programa, incluyendo las medidas de seguridad, que prevea una revisión cada tres años o antes si es necesario por un cambio sustancial en el tratamiento.	Comité de Transparencia.	• Programa de supervisión y vigilancia, y resultados obtenidos.
Establecer procedimientos para recibir y responder dudas y quejas de los titulares, que sea de fácil acceso y con la mayor cobertura posible; considerando el perfil de los titulares y la forma en que se mantiene contacto o comunicación directa o cotidiana con ellos, así como estar, en todo momento, habilitado.	5. Establecer un procedimiento para atender dudas y quejas de los titulares con las características señaladas en la columna anterior.	Comité y Unidad de Transparencia.	• Procedimiento establecido.
Implementar mecanismos para evidenciar el cumplimiento de los principios, deberes y obligaciones ante los titulares y el Instituto, tanto de tratamiento propio como de aquéllos realizados por los encargados y en las transferencias nacionales e internacionales.	7. En todos los casos generar pruebas para acreditar el cumplimiento de los principios, deberes y obligaciones que establece la LGPDPPSO, los Lineamientos Generales y demás disposiciones que resulten aplicables.	Unidades administrativas del CENAPRED, Comité de Transparencia y Unidad de Transparencia.	• Pruebas generadas según lo establecido en la columna de “Medios para acreditar el cumplimiento” de todos los cuadros de este Programa.

Artículos vinculados: 29 y 30 de la LGPDPPSO y 46 al 54 de los Lineamientos Generales.

Comprobación:	**Sí**	**No**

Programa de Protección de Datos Personales

El presupuesto del CENAPRED contempla los recursos públicos necesarios o posibles para la instrumentación de programas y políticas de protección de datos personales.	☐	☐
Se tiene y aplica un programa de protección de datos personales que es de cumplimiento obligatorio al interior del CENAPRED.	☐	☐
Se tiene y aplica un programa de capacitación y actualización de los servidores públicos en materia de protección de datos personales según lo establecido en este Programa.	☐	☐
Se tiene y aplica un procedimiento y programa de supervisión y vigilancia y/o externa para comprobar el cumplimiento de este programa, incluyendo las medidas de seguridad, cada dos años o antes si es necesario.	☐	☐
Se tiene y aplica un procedimiento para atender dudas y quejas de los titulares.	☐	☐
Las políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología, que implique el tratamiento de datos personales, se diseñan, desarrollan e implementan tomando en cuenta la privacidad por diseño y por defecto.	☐	☐
Se generan pruebas para acreditar el cumplimiento de los principios, deberes y obligaciones que establece la LGPDPPSO, los Lineamientos Generales y demás disposiciones que resulten aplicables.	☐	☐

5. FUNCIONES DEL COMITÉ DE TRANSPARENCIA DEL CENAPRED

Obligaciones	**Actividades para su cumplimiento**	**Unidad administrativa responsable del cumplimiento**	**Medios para acreditar el cumplimiento**
El Comité de Transparencia será la autoridad máxima en materia de protección de datos personales al interior del CENAPRED, y al respecto, tendrá las siguientes funciones: Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en el INAI, de conformidad con las disposiciones previstas en la LGPDPPSO y en aquellas disposiciones que resulten aplicables en la materia; Instituir, en su caso, procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO; Confirmar, modificar o revocar las determinaciones en las que se declare la	1. Establecer un programa de trabajo para la implementación del Programa. 2. Supervisar la debida implementación del Programa por parte de las unidades administrativas del CENAPRED y realizar las modificaciones o mejoras al mismo que resulten pertinentes. 3. Establecer un procedimiento para	Comité de Transparencia.	• Programas establecidos e implementados.

Programa de Protección de Datos Personales

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
inexistencia de los datos personales, o se niegue por cualquier causa el ejercicio de alguno de los derechos ARCO; 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; Supervisar, en coordinación con las unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad; Dar seguimiento y cumplimiento a las resoluciones emitidas por el INAI; Establecer programas de capacitación y actualización para los servidores públicos en materia de protección de datos personales, y 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.	supervisar el cumplimiento de las medidas de seguridad, controles y acciones previstos en el documento de seguridad. 4. Establecer un programa de capacitación y actualización para los servidores públicos, en materia de protección de datos personales.		

Artículos vinculados: 83 y 84 de la LGPDPPSO.

Comprobación:	**Sí**	**No**
1. Se cuenta con un Comité de Transparencia.	☐	☐
2. Se cuenta con un programa de trabajo para la implementación del Programa de Protección de Datos Personales.	☐	☐
3. Se realizan acciones de supervisión de la implementación del Programa.	☐	☐
4. Se cuenta con un procedimiento para supervisar el cumplimiento del documento de seguridad.	☐	☐

Programa de Protección de Datos Personales

Se cuenta con un programa de capacitación y actualización para los servidores públicos, en materia de protección de datos personales.	☐	☐

6. FUNCIONES DE LA UNIDAD DE TRANSPARENCIA DEL CENAPRED

Obligaciones	**Actividades para su cumplimiento**	**Unidad administrativa responsable del cumplimiento**	**Medios para acreditar el cumplimiento**
La Unidad de Transparencia tendrá las siguientes funciones en materia de protección de datos personales: Auxiliar y orientar al titular que lo requiera con relación al ejercicio del derecho a la protección de datos personales; Gestionar las solicitudes para el ejercicio de los derechos ARCO; Establecer mecanismos para asegurar que los datos personales solo se entreguen a su titular o su representante debidamente acreditados; 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; 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; Aplicar instrumentos de evaluación de calidad sobre la gestión de las solicitudes para el ejercicio de los derechos ARCO, y Asesorar a las unidades administrativas en materia de protección de datos personales.	1. Establecer procedimientos internos para cumplir con sus funciones y para gestionar de manera eficiente las solicitudes de derechos ARCO. 2. Diseñar la metodología y programa de evaluaciones de calidad sobre la gestión de las solicitudes de ejercicio de los derechos ARCO, y aplicar dichas evaluaciones.	Unidad de Transparencia.	• Procedimientos y programas establecidos e implementados.
Auxiliar y orientar al titular en la elaboración de las solicitudes para el ejercicio de sus derechos ARCO, en todo momento, y en especial en aquellos casos en que el titular no sepa leer ni escribir, así como informar sobre la obligación del titular de acreditar su identidad y, en su	3. Auxiliar y orientar a los titulares en las presentaciones de sus solicitudes de ejercicio de derechos ARCO.	Unidad de Transparencia.	• Procedimientos y programas establecidos e implementados.

Programa de Protección de Datos Personales

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
caso, la identidad y personalidad de su representante. Para el caso de las personas con alguna discapacidad, la Unidad de Transparencia procurará atender a cada uno de los titulares, de acuerdo con su situación particular, facilitando en todo momento la información que éstos requieran para el ejercicio de sus derechos ARCO.			

Artículos vinculados: 85 y 87 de la LGPDPPSO.

Comprobación:	Sí	No
1. Se cuenta con una Unidad de Transparencia.	☐	☐
2. Se cuenta con procedimientos internos para realizar las funciones y gestionar de manera eficiente las solicitudes de derechos ARCO y auxiliar y orientar a los titulares en la presentación de las solicitudes.	☐	☐
3. Se cuenta con una metodología para la aplicación de evaluaciones de calidad sobre la gestión de las solicitudes de ejercicio de derechos ARCO.	☐	☐

7. CAPACITACIÓN

Como parte de las actividades interrelacionadas también se encuentra la capacitación, el diseñar e implementar programas a corto, mediano y largo plazo, para los involucrados en el tratamiento de los datos personales, atendiendo a sus roles, funciones y responsabilidades asignados.

Por lo tanto, a fin de contar con personal consciente de sus responsabilidades y deberes respecto de la protección de datos personales, se deben establecer y mantener programas de capacitación considerando las siguientes etapas:

1. **Concienciación:** programas a corto plazo para la difusión en general de la protección de datos personales en la organización.

2. **Entrenamiento:** programas a mediano plazo que tienen por objetivo capacitar al personal de manera específica respecto a sus funciones y responsabilidades en el tratamiento y seguridad de los datos personales.

3. **Educación:** programa general a largo plazo que tiene por objetivo incluir la seguridad en el tratamiento de los datos personales dentro de la cultura de la organización.

Programa de Protección de Datos Personales

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
Establecer 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 considerar los roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales y el perfil de puestos.	1. Establecer un programa anual de capacitación y actualización en materia de protección de datos personales para los servidores públicos y encargados.	Comité de Transparencia a través dl enlace de capacitación del CENAPRED.	• Programa anual de capacitación.

El programa de capacitación formará parte de este Programa.

Artículos vinculados: 92 de la LGPDPPSO 48 y 64 de los Lineamientos Generales.

Comprobación:	Sí	No
1. Se cuenta con un programa anual de capacitación y actualización de los servidores públicos y encargados de la protección de los datos personales, que toma en cuenta los roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales y el perfil de puestos.	☐	☐

8. Sanciones por incumplimiento al Programa

Cuando el Comité de Transparencia del CENAPRED tenga conocimiento del incumplimiento de alguna obligación prevista en este Programa, deberá realizar a la unidad administrativa correspondiente un exhorto para que lleve a cabo las acciones que resulten pertinentes con objeto de modificar dicha situación y evitar incumplimientos futuros o situaciones de riesgo que los pudieran ocasionar.

Adicionalmente, a través de este instrumento, se hace del conocimiento a todas las personas servidoras públicas del CENAPRED que están a cargo del tratamiento de datos personales, que de conformidad con el artículo 163 de la LGPDPPSO serán causas de sanción por incumplimiento de las obligaciones establecidas en dicha 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 LGPDPPSO 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 LGPDPPSO;

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 LGPDPPSO, 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 LGPDPPSO;

VIII. No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la LGPDPPSO;

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 LGPDPPSO;

X. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la LGPDPPSO;

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 LGPDPPSO;

XIII. No acatar las resoluciones emitidas por el INAI, 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, serán consideradas como graves.

Asimismo, de conformidad con el artículo 105 de los Lineamientos Generales, cuando alguna unidad administrativa del CENAPRED se niegue a colaborar con la Unidad de Transparencia en la atención de las solicitudes para el ejercicio de los derechos ARCO, ésta dará aviso al superior jerárquico 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, contraloría o instancia equivalente y, en su caso, dé inicio el procedimiento de responsabilidad administrativo respectivo.

Cabe destacar que las sanciones de carácter económico no podrán ser cubiertas con recursos públicos.

Las responsabilidades que resulten de los procedimientos administrativos correspondientes, son independientes de las del orden civil, penal o de cualquier otro tipo que se puedan derivar de los mismos hechos.

El Comité de Transparencia tomará las medidas necesarias para que las personas servidoras públicas del CENAPRED conozcan esta información.

9. Vigencia y Aprobación

El presente Programa entrará en vigor el día siguiente de su aprobación por el Comité de Transparencia del CENAPRED.

Programa de Protección de Datos Personales

El presente documento fue aprobado por unanimidad por el Comité de Transparencia del CENAPRED en su Segunda Sesión Ordinaria del 6 de abril de 2022 de conformidad con los artículos 30, 83 y 84 de la LGDPPSO.

Lic. Claudia Núñez Peredo
Directora de Servicios Técnicos y
Titular de la Unidad de Transparencia

Lic. Rubén Michele Gutiérrez Gudiño
Subdirector de Enlace Interinstitucional y
Responsable del Archivo de Trámite

Lic. Luis Jesús Moreno Velázquez
Titular del Área de Responsabilidades, en representación del Titular del Órgano Interno de Control
Secretaría de Función la Pública.

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Unidad administrativa:	Señalar nombre de la unidad administrativa a cargo o administradora del proceso o procedimiento en el que se tratan los datos personales.
Fecha de elaboración o última actualización:	Señalar fecha en la que concluyó la elaboración del inventario o su última actualización
Nombre del tratamiento (proceso):	Señalar nombre del tratamiento.
Fundamento jurídico que habilita el tratamiento:	Señalar las principales disposiciones
Atribuciones de la unidad administrativa para realizar el tratamiento:	Señalar las atribuciones específicas de la unidad administrativa para llevar a cabo el tratamiento, entre ellas, las que señala el Reglamento o Estatuto Orgánico interno, y otras si las hubiere.

Medio de obtención de los datos personales (1)			Tercero que transfiere los datos personales, en su caso (2)	Finalidades de la transferencia recibida, en su caso (3)	Listado de datos personales (4)		Sensible (5)	Formato de la base de datos (6)
Señalar el o los medios a través de los cuales se obtienen los datos personales en este tratamiento. Si es más de un medio, se deberá indicar un medio por fila.	Describir el medio, por ejemplo la fuente de acceso público, URL, domicilio, número telefónico, entre otros	En caso de seleccionar la opción otro, especificar el medio de obtención.	Si en la columna 1 se indicó que los datos personales se reciben por transferencia, señalar el nombre del tercero o terceros que realizan la transferencia.	Si en la columna 1 se indicó que los datos personales se reciben por transferencia, señalar para qué finalidades se realiza dicha transferencia. Se deberá utilizar la misma fila por tercero que transfiere los datos personales.	Indicar cada uno de los datos personales que se tratan o sus categorías, uno por fila.	En caso de seleccionar la opción otro, especificar.	Señalar si el dato personal es sensible o no.	Señalar el o los formatos en los que se encuentra la base de datos del tratamiento.

Ubicación base de datos (7)		Sección de archivos (8)	Serie de archivos (9)	Subserie de archivos (10)	Finalidades del tratamiento (11)	¿Requiere consentimiento? (12)	Supuesto artículo 22 que se actualiza, en su caso (13)	Tipo de consentimiento (14)	Servidores públicos que tienen acceso a la base de datos (15)
Señalar la ubicación de la base de datos. Si es más de uno, se deberá indicar uno por fila.	En caso de seleccionar la opción otro, especificar la ubicación.	Indicar clave de identificación de la sección a la que corresponde el tratamiento.	Indicar clave de identificación de la serie a la que corresponde el tratamiento.	Indicar clave de identificación de la subserie a la que corresponde el tratamiento.	Indicar cada una de las finalidades del tratamiento, las cuales deberán ser explícitas y concretas. Una por fila.	Indicar si la finalidad requiere o no el consentimiento del titular.	En caso de que la finalidad no requiera el consentimiento del titular, señalar el o los supuestos del artículo 22 de la LGPDPPSO que se actualizan.	En caso de que la finalidad requiera el consentimiento del titular, señalar el tipo de consentimiento que se necesita.	Señalar los puestos de los servidores públicos que tienen acceso a la base de datos del tratamiento correspondiente. Uno por fila.

Área de adscripción (16)	Finalidad del acceso (17)	Nombre del encargado, en su caso (18)	No. de contrato, pedido o convenio con el encargado, o del instrumeto jurídico correspondiente (19)	¿Se realizan transferencias? (20)	Tercero al que se transfieren los datos personales, en su caso (21)	Finalidades de la transferencia (22)	¿Requiere consentimiento la transferencia? (23)	Supuestos artículos 22, 66 o 70 que se actualizan, en su caso (24)	Tipo de consentimiento que se requiere para la transferencia (25)
Definir unidad administrativa a la que está adscrito el puesto	Señalar con qué fines tienen acceso los servidores públicos antes identificados. Uno por fila, según corresponda.	Señalar nombre de la o las personas físicas o morales que actúan como encargados en el tratamiento, en su caso. Uno por fila.	Señalar el número de identificación del instrumento jurídico que regula la relación con el encargado.	Señalar si se realizan o no transferencias en el marco del tratamiento.	Señalar el nombre, razón o denominación social de los terceros a los que se transfieren los datos personales, cuando ello sea posible, o bien, su categoría. Uno por fila.	Señalar las finalidades para las cuales se transfieren los datos personales por cada uno de los terceros.	Señalar si la transferencia requiere o no consentimiento.	En caso de que la transferencia no requiera consentimiento, señalar los supuestos que se actualizan.	En caso de que la finalidad de la transferencia requiera el consentimiento del titular, señalar si se requiere el tácito o el expreso y por escrito.

¿La transferencia requiere la suscripción de cláusulas contractuales, convenios de colaboración u otro instrumento jurídico? (26)	Supuesto artículo 66 que se actualiza, en su caso (27)	Difusión de los datos personales (28)	Fundamento jurídico para la difusión (29)	Plazo de conservación (30)	Bloqueo (31)	Observaciones
Indicar si la transferencia requiere de la suscripción de cláusulas contractuales, convenios de colaboración u otro instrumento jurídico, según el artículo 66 de la LGPDPPSO	Señalar el supuesto que en su caso se actualiza, si no se requiere de la suscripción de cláusulas contractuales, convenios de colaboración u otro instrumento	Indicar si en el tratamiento se realiza la difusión de los datos personales.	Indicar el fundamento jurídico que ordena la difusión de los datos personales.	Señalar el plazo de conservación de los datos personales, según lo señalado en los instrumentos de clasificación archivística	Señalar periodo en el que estarán bloquedos los datos personales.	Espacio libre para hacer aclaraciones y precisiones

ANEXO 2
1.T. MEDIDAS DE SEGURIDAD (DEBER DE SEGURIDAD)
2.T. DOCUMENTO DE SEGURIDAD

1. ¿En qué consiste el deber de seguridad?

El deber de seguridad consiste en la implementación de medidas de seguridad físicas, técnicas y administrativas necesarias para proteger los datos personales contra daño, pérdida, alteración, destrucción, o su uso, acceso o tratamiento no automatizado, así como para garantizar su confidencialidad, integridad y disponibilidad.

Las medidas de seguridad son el conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.

Las medidas de **seguridad administrativas** refieren a las 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.

Por su parte, las medidas de **seguridad físicas** son el 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.

Asimismo, las medidas de **seguridad técnicas** abarcan el 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.

Este deber deberá observarse durante todo el ciclo de vida de los datos personales, desde su obtención hasta su eliminación.

Por otra parte, de conformidad con el artículo 35 de la LGPDPPSO, el responsable deberá elaborar un documento de seguridad, el cual deberá contener, al menos, la siguiente información:

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

2. ¿Cuáles son las obligaciones vinculadas con el deber de seguridad?

2.1 Generales:

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
• Establecer y mantener medidas de seguridad de carácter administrativo, físico y técnico, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad e impedir que cualquier tratamiento contravenga las disposiciones del marco normativo en la materia.	1. Establecer y mantener medidas de seguridad administrativas, técnicas y físicas para la protección de los datos personales, a partir de las acciones que se describen en esta sección.	La Coordinación Administrativa en conjunto con la Dirección de Instrumentación y Cómputo del CENAPRED en el ámbito de sus atribuciones, con la participación de las unidades administrativas.	• Programa de Protección de Datos Personales. • Documento de seguridad. • Evidencia generada en la implementación de los controles de seguridad.
• Tomar en cuenta otras	2. Revisar el marco normativo	Unidad administrativa	• Marco normativo que

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
disposiciones vigentes en materia de seguridad de la información emitidas por otras autoridades, cuando éstas contemplen una mayor protección para el titular o complementen lo dispuesto por la LGPDPPSO y los Lineamientos Generales.	que regula el tratamiento específico de los datos personales, a fin de identificar medidas de seguridad adicionales y analizar la procedencia de su implementación.	responsable del tratamiento con el apoyo de la Coordinación Administrativa y la Dirección de Instrumentación y Cómputo del CENAPRED .	regula en lo particular el tratamiento en cuestión.

2.2 Políticas internas:

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
• Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión, y en las que se incluya lo siguiente: I. El cumplimiento de todos los principios, deberes, derechos y demás obligaciones en la materia, de conformidad con lo previsto en la LGPDPPSO y los presentes Lineamientos generales; II. Los roles y responsabilidades específicas de los involucrados internos y externos dentro de su organización, relacionados con los tratamientos de datos personales que se efectúen; III. Las sanciones en caso de incumplimiento; IV. La identificación del	3. Incluir en el Programa de Protección de Datos Personales los elementos señalados en la columna anterior.	Comité de Transparencia.	• Programa de Protección de Datos Personales, según la sección 4. • Documentación que se genere con motivo de la implementación y evaluación del Programa.

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
ciclo de vida de los datos personales respecto de cada tratamiento que se efectúe; considerando la obtención, almacenamiento, uso, procesamiento, divulgación, retención, destrucción o cualquier otra operación realizada durante dicho ciclo en función de las finalidades para las que fueron recabados; V. El proceso general para el establecimiento, actualización, monitoreo y revisión de los mecanismos y medidas de seguridad; considerando el análisis de riesgo realizado previamente al tratamiento de los datos personales, y VI. El proceso general de atención de los derechos ARCO.			

2.3 Funciones de los servidores públicos que tratan datos personales:

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
• Establecer y documentar las funciones, obligaciones y cadena de rendición de cuentas del personal involucrado en el tratamiento de datos personales. • Establecer mecanismos para asegurar que los servidores públicos involucrados en el tratamiento conozcan sus funciones para el cumplimiento de los objetivos del sistema de gestión, así como las consecuencias de su incumplimiento.	4. Definir las funciones, obligaciones y cadena de mando de cada servidor público que trate datos personales, por unidad administrativa. 5. Comunicar a cada uno de los servidores públicos la información antes señalada, así como capacitarlos en la materia.	Unidad administrativa responsable del tratamiento.	• Documento en el que se establezcan las funciones, obligaciones y cadena de mando de cada servidor público, por unidad administrativa, que trate datos personales según el apartado 2 y 4 de este Programa. • Documento mediante el cual se haya comunicado la información antes señalada. • Constancias de capacitación al personal.

2.4 Inventario:

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
• Elaborar un inventario de datos personales y de los sistemas de tratamiento, en el que se incluyan los siguientes elementos: I. El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales; II. Las finalidades de cada tratamiento de datos personales; III. El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no; IV. El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales; V. La lista de servidores públicos que tienen acceso a los sistemas de tratamiento; VI. En su caso, el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la	6. Elaborar el inventario de datos personales y de los sistemas de tratamiento con los elementos señalados en la columna anterior.	Comité de Transparencia en conjunto con las unidades administrativas encargadas del tratamiento.	• Inventario de tratamiento de datos personales según el apartado 4.1 de este Programa.

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
prestación de los servicios que brinda al responsable, y VII. En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que las justifican. • Considerar en el inventario el ciclo de vida de los datos personales, conforme a lo siguiente: I. La obtención de los datos personales; II. El almacenamiento de los datos personales; III. El uso de los datos personales conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin; IV. La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen; V. El bloqueo de los datos personales, en su caso,			

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
y VI. La cancelación, supresión o destrucción de los datos personales.			

2.5 Análisis de riesgo, de brecha y plan de trabajo:

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
• Realizar un análisis de riesgo de los datos personales, considerando lo plasmado en la Política de Seguridad en Datos Personales en el CENAPRED o en su caso si aplican en lo conducente se observará lo siguiente: I. Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico; II. El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida; III. El valor y exposición de los activos involucrados en el tratamiento de los datos personales; IV. Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida; V. El riesgo inherente a los datos personales tratados, contemplando el ciclo de vida de los datos personales, las	7. Elaborar el análisis de riesgo tomando en cuenta los elementos señalados en la columna anterior.	La participación de las unidades administrativas en coordinación con la Dirección de Instrumentación y Cómputo y la Coordinación Administrativa del CENAPRED quienes darán el visto bueno.	• Análisis de riesgo documentado. • Documento de seguridad.

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
amenazas y vulnerabilidades existentes para los datos personales y los recursos o activos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal o cualquier otro recurso humano o material, entre otros; VI. La sensibilidad de los datos personales tratados; VII. El desarrollo tecnológico; VIII. Las transferencias de datos personales que se realicen; IX. El número de titulares; X. Las vulneraciones previas ocurridas en los sistemas de tratamiento, y XI. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.			
• Realizar un análisis de brecha, comparando las	8. Realizar el análisis de brecha con los elementos	La participación de las unidades administrativas en	• Análisis de brecha documentado.

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
medidas de seguridad existentes contra las faltantes en la organización del responsable, considerando lo siguiente: I. Las medidas de seguridad existentes y efectivas; II. Las medidas de seguridad faltantes, y III. La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.	señalados en la columna anterior.	coordinación con la Dirección de Instrumentación y Cómputo y la Coordinación Administrativa del CENAPRED quienes darán el visto bueno.	• Documento de seguridad.
• Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales. Este plan de trabajo deberá elaborarse de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer. Lo anterior, considerando los recursos designados; el	9. Elaborar el plan de trabajo después de contar con el análisis de riesgo y de brecha, priorizando las medidas de seguridad más relevantes y urgentes, considerando los recursos designados; el personal interno y externo en su organización, y estableciendo fechas compromiso para la implementación de las medidas de seguridad nuevas o faltantes.	La Coordinación Administrativa y la Dirección de Instrumentación y Cómputo del CENAPRED con la participación de las unidades administrativas.	• Plan de trabajo elaborado. • Documentos de análisis de riesgo y de brecha.

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
personal interno y externo en su organización y las fechas compromiso para la implementación de las medidas de seguridad nuevas o faltantes.			

2.6 Revisión y vigilancia:

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
• Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, tomando en cuenta lo siguiente: I. Los nuevos activos que se incluyan en la gestión de riesgos; II. Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras; III. Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas; IV. La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes; V. Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que	10. Elaborar un plan de monitoreo periódico de las medidas de seguridad implementadas, las amenazas y las vulnerabilidades a las que estén sujetos los datos personales, tomando en cuenta los elementos señalado en la columna anterior. 11. Implementar el plan de monitoreo periódico.	La Coordinación Administrativa y la Dirección de Instrumentación y Cómputo del CENAPRED, con la participación de las unidades administrativas.	• Plan de monitoreo periódico. • Documentación que se genere a partir de la implementación del plan.

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
vuelvan a surgir; VI. El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y VII. Los incidentes y vulneraciones de seguridad ocurridas.			

3.7 Capacitación:

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
• Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales, seguridad de los datos personales y el perfil de los puestos.	12. Realizar las acciones previstas en el apartado de "Capacitación".	Comité de Transparencia.	• Programa de capacitación. • Documentación que se genere a partir de la aplicación de la capacitación.

2.8 Sistema de gestión:

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
• Implementar un sistema de gestión para la seguridad de los datos personales, que permita planificar, establecer, implementar, operar, monitorear, mantener, revisar y mejorar las medidas de seguridad de carácter administrativo, físico y técnico aplicadas a los datos personales; tomando en consideración los estándares nacionales e internacionales en materia de protección de datos personales y seguridad.	13. Implementar el presente Programa de Protección de Datos Personales que se basa en un sistema de gestión integral, que no sólo abarca medidas de seguridad sino la totalidad de obligaciones previstas en la LGPDPPSO y los Lineamientos Generales.	Comité de Transparencia, La Coordinación Administrativa y la Dirección de Instrumentación y Cómputo del CENAPRED, y las unidades administrativas.	• Programa de Protección de Datos Personales. • Documentación que se genere a partir de la implementación del Programa.

2.9 Documento de seguridad:

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento

• Elaborar un documento de seguridad con la siguiente información:
  • El inventario de datos personales y de los sistemas de tratamiento;
  • Las funciones y obligaciones de las personas que traten datos personales;
  • El análisis de riesgos;
  • El análisis de brecha;
  • El plan de trabajo;
  • Los mecanismos de monitoreo y revisión de las medidas de seguridad, y
  • El programa general de capacitación.
	14. Elaborar el documento de seguridad con la información antes señalada.	Se valorará de acuerdo a los resultados obtenidos, si se hará un documento por cada unidad administrativa o uno en general para el CENAPRED, en cuyo caso las unidades responsables, serían la Coordinación Administrativa y la Dirección de Instrumentación y Cómputo con la participación de las demás unidades administrativas.	• Documento de seguridad.

• Actualizar el documento de seguridad cuando ocurran los siguientes eventos:
  ○ Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;
  ○ Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;
	15. Actualizar el documento de seguridad cuando ocurra alguno de los supuestos antes señalados.	Será aplicable el supuesto anterior.	• Documento de seguridad.

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
○ Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida, e ○ Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.			

3. Lista de comprobación

	Sí	No
1. Se han definido y se establecen y mantienen las medidas de seguridad administrativas, técnicas y físicas necesarias para la protección de los datos personales.	☐	☐
2. Se ha revisado el marco normativo que regula en lo particular el tratamiento de datos personales en cuestión, a fin de identificar si éste contempla medidas de seguridad específicas o adicionales a las previstas en la LGPDPPSO y los Lineamientos Generales, y se ha definido la procedencia de su implementación.	☐	☐
3. El Programa de Protección de Datos Personales de la organización toma en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, e incluye lo siguiente: • El cumplimiento de todos los principios, deberes, derechos y demás obligaciones en la materia, de conformidad con lo previsto en la LGPDPPSO y los presentes Lineamientos generales; • Los roles y responsabilidades específicas de los involucrados internos y externos dentro de su organización, relacionados con los tratamientos de datos personales que se efectúen; • Las sanciones en caso de incumplimiento; • La identificación del ciclo de vida de los datos personales respecto de cada tratamiento que se efectúe; considerando la obtención, almacenamiento, uso, procesamiento, divulgación, retención, destrucción o cualquier otra operación realizada durante dicho ciclo en función de las finalidades para las que fueron recabados; • El proceso general para el establecimiento, actualización, monitoreo y revisión de los mecanismos y medidas de seguridad; considerando el análisis de riesgo realizado previamente al tratamiento de los datos personales, y El proceso general de atención de los derechos ARCO.	☐	☐
3. Se han definido las funciones, obligaciones y cadena de mando de cada servidor público que trata datos personales, por unidad administrativa.	☐	☐
4. Se ha comunicado a cada servidor público sus funciones, obligaciones y cadena de mando con relación al tratamiento de datos personales que efectúa.	☐	☐
5. Se ha elaborado el inventario de datos personales con los siguientes elementos: • El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales; • Las finalidades de cada tratamiento de datos personales; • El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no; • El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales; • La lista de servidores públicos que tienen acceso a los sistemas de tratamiento; • En su caso, el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable, y • En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que las justifican.	☐	☐
6. En el inventario de datos personales se tomó en cuenta el ciclo de vida de los datos personales, conforme	☐	☐

a lo siguiente: • La obtención de los datos personales; • El almacenamiento de los datos personales; • El uso de los datos personales conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin; • La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen; • El bloqueo de los datos personales, en su caso, y • La cancelación, supresión o destrucción de los datos personales.		
7. Se ha realizado el análisis de riesgo, considerando lo siguiente: • Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico; • El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida; • El valor y exposición de los activos involucrados en el tratamiento de los datos personales; • Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida; • El riesgo inherente a los datos personales tratados, contemplando el ciclo de vida de los datos personales, las amenazas y vulnerabilidades existentes para los datos personales y los recursos o activos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal o cualquier otro recurso humano o material, entre otros; • La sensibilidad de los datos personales tratados; • El desarrollo tecnológico; • Las transferencias de datos personales que se realicen; • El número de titulares; • Las vulneraciones previas ocurridas en los sistemas de tratamiento, y • El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.	☐	☐
8. Se ha realizado el análisis de brecha, tomando en cuenta lo siguiente: • Las medidas de seguridad existentes y efectivas; • Las medidas de seguridad faltantes, y • La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.	☐	☐
9. Se ha elaborado el plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales, a partir del análisis de riesgo y brecha realizado, y priorizando las medidas de seguridad más relevantes e inmediatas a establecer.	☐	☐
10. Se monitorea y revisa de manera periódica s medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, tomando en cuenta lo siguiente: • Los nuevos activos que se incluyan en la gestión de riesgos; • Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica,	☐	☐

entre otras; • Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas; • La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes; • Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir; • El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y • Los incidentes y vulneraciones de seguridad ocurridas.		
11. Se cuenta con un programa de capacitación para los servidores públicos y externos involucrados en el tratamiento de datos personales, y se implementa.	☐	☐
12. Se implementa un sistema de gestión para la seguridad de los datos personales.	☐	☐
13. Se cuenta con el documento de seguridad con la información que establece el artículo 35 de la LGPDPPSO.	☐	☐
14. En el documento de seguridad se establece un procedimiento para su actualización, en caso de que ocurra alguno de los supuestos del artículo 36 de la LGPDPPSO.	☐	☐

ANEXO 3
3.T. VULNERACIONES

1. ¿Qué es una vulneración de datos personales?

Además de las que señalen las leyes respectivas y la normatividad aplicable, se considerarán como vulneraciones de seguridad, en cualquier fase del tratamiento de datos, al menos, las siguientes:

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

2. ¿En qué artículos de la Ley General y de los Lineamientos se prevé lo relativo a las vulneraciones?

37 al 41 de la LGPDPPSO y 66 a 68 de los Lineamientos Generales.

3. ¿Cuáles son las obligaciones vinculadas con las vulneraciones?

3.1 Notificación de la vulneración: casos y plazo:

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
• Informar al titular y al INAI, las vulneraciones que afecten de forma significativa los derechos patrimoniales o morales, en un plazo máximo de 72 horas, a partir de que se confirme que ocurrió la vulneración y que se haya empezado a tomar las acciones encaminadas a detonar un proceso de mitigación de la afectación. El plazo de 72 horas comenzará a correr el mismo día natural en que el	1. Contar con mecanismos que permitan identificar cuándo ocurrió una vulneración a las bases de datos o archivos.	• La Dirección de Instrumentación y Cómputo con la participación de todas las Unidades Administrativas del CENAPRED involucradas en la seguridad de la información en lo relativo a sistemas electrónicos. • La Coordinación Administrativa del CENAPRED y unidad administrativa responsable de la base de datos correspondiente, en archivos físicos.	• Mecanismos implementados para detectar vulneraciones ocurridas. • Procedimiento para la gestión de vulneraciones de datos personales

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
responsable confirme la vulneración de seguridad. Se entenderá que se afectan los derechos patrimoniales del titular cuando la vulneración esté 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. Se entenderá que se afectan los derechos morales del titular cuando la vulneración esté 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.	2. Establecer un procedimiento para notificar las vulneraciones ocurridas al titular y al INAI en el plazo de 72 horas.	• Comité de Transparencia y las unidades administrativas del CENAPRED encargadas de la seguridad de la información al interior de la institución.	

3.2 Contenido de informe para el titular:

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
• Informar al titular lo siguiente con relación a la vulneración ocurrida: o La naturaleza del incidente o vulneración ocurrida; o Los datos personales comprometidos; o Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses; o Las acciones correctivas realizadas de forma inmediata; o Los medios donde puede obtener más información al respecto; o La descripción de las circunstancias generales en torno a la vulneración ocurrida, que ayuden al titular a entender el impacto del incidente, y o Cualquier otra información y documentación que considere conveniente para apoyar a los titulares.	3. Elaborar un formato de notificación de las vulneraciones de seguridad ocurridas, donde se incluya la información a la que refiere la columna anterior.	• Comité de Transparencia.	• Formato de notificación al titular de la vulneración de seguridad ocurrida. • Constancia de las notificaciones.
	4. Realizar las notificaciones de las vulneraciones cuando éstas ocurran, en el momento y con la información antes señalada.	• Unidad administrativa responsable de la base de datos o archivo que fue vulnerado, con notificación al Comité de Transparencia.	

3.3 Contenido de informe para el INAI:

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
• Informar al Instituto la siguiente información: I. La hora y fecha de la identificación de la vulneración; II. La hora y fecha del inicio de la investigación sobre la vulneración; III. La naturaleza del incidente o vulneración ocurrida; IV. La descripción detallada de las circunstancias en torno a la vulneración ocurrida; V. Las categorías y número aproximado de titulares afectados; VI. Los sistemas de tratamiento y datos personales comprometidos; VII. Las acciones correctivas	5. Elaborar un formato de notificación de las vulneraciones de seguridad ocurridas, donde se incluya la información a la que refiere la columna anterior.	• Comité de Transparencia.	• Formato de notificación al Instituto de la vulneración de seguridad ocurrida. • Constancia de las notificaciones.

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
realizadas de forma inmediata; VIII. La descripción de las posibles consecuencias de la vulneración de seguridad ocurrida; IX. Las recomendaciones dirigidas al titular; X. El medio puesto a disposición del titular para que pueda obtener mayor información al respecto; XI. El nombre completo de la o las personas designadas y sus datos de contacto, para que puedan proporcionar mayor información al Instituto, en caso de requerirse, y XII. Cualquier otra información y documentación que considere conveniente hacer del conocimiento del Instituto.	6. Realizar las notificaciones de las vulneraciones cuando éstas ocurran, en el momento y con la información antes señalada.	• Unidad administrativa responsable de la base de datos o archivo que fue vulnerado, con notificación al Comité de Transparencia.	

3.4 Medios de notificación:

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
• Determinar los medios por los cual se notificará a los titulares las vulneraciones ocurridas, tomando en cuenta lo siguiente: el perfil de los titulares, la forma en que mantiene contacto o comunicación con éstos, que sean gratuitos; de fácil acceso; con la mayor cobertura posible y que estén debidamente habilitados y disponibles en todo momento para el titular.	7. Determinar los medios de notificación de las vulneraciones.	• Unidad administrativa responsable de la base de datos o archivo que fue vulnerado.	• Documento en el que se describan los medios que se utilizarán en caso de que sea necesario notificar vulneraciones. • Medio utilizado para notificar la vulneración.

3.5 Bitácora:

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
• Llevar una bitácora de las vulneraciones de seguridad ocurridas, en la que se describa la vulneración, la fecha en la que ocurrió, el motivo de ésta y las acciones correctivas implementadas de forma inmediata y definitiva.	8. Elaborar un formato de bitácora de las vulneraciones ocurridas con la información antes señalada. 9. Llevar una la bitácora de las vulneraciones de seguridad ocurridas.	• Comité de Transparencia.	• Bitácoras.

3.6 Acciones preventivas y correctivas:

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
• Analizar las causas por las cuales se presentó la vulneración e implementar en el plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales, a fin de evitar que la vulneración se repita.	10. Identificar y documentar las posibles causas de la vulneración e implementar las acciones preventivas y correctivas que se requieran para evitar que se repita. 11. Informar al Comité de Transparencia las acciones implementadas para evitar que se repita la vulneración.	• Todas las Unidades Administrativas del CENAPRED encargadas de la seguridad de la información al interior de la institución, en lo relativo a sistemas electrónicos. • Unidades administrativas encargadas de la seguridad, en archivos físicos.	• Análisis realizado. • Acciones implementadas. • Informe al Comité de Transparencia.

4. Lista de comprobación

	Sí	No
Se cuenta con mecanismos que permitan identificar las vulneraciones ocurridas a las distintas bases de datos y archivos del sujeto obligado.	☐	☐
Se cuenta con el procedimiento para realizar notificaciones de vulneraciones tanto a los titulares como al INAI.	☐	☐
Se han elaborado los formatos para notificar las vulneraciones a los titulares y al INAI, respectivamente.	☐	☐
Se han determinado los medios para notificar las vulneraciones.	☐	☐
Se han realizado las notificaciones de las vulneraciones en el momento y con la información establecida por la LGPDPPSO y los Lineamientos Generales.	☐	☐
Se cuenta con una bitácora de las vulneraciones ocurridas.	☐	☐
Se han identificado las causas de las vulneraciones e implementado las acciones preventivas y correctivas que se requieran para evitar que se repita.	☐	☐
Se ha informado al Comité de Transparencia sobre las acciones preventivas y correctivas implementadas para evitar que se repita la vulneración.	☐	☐