POLÍTICA INTERNA

DE PROTECCIÓN DE DATOS PERSONALES DEL CENTRO NACIONAL DE PREVENCIÓN DE DESASTRES

Unidad de Transparencia

Abril 2022

Política Interna de Protección de Datos Personales

ÍNDICE

Política Interna de Protección de Datos Personales

INTRODUCCIÓN

El Centro Nacional de Prevención de Desastres, (CENAPRED) es un Órgano Administrativo Desconcentrado de la Secretaría de Seguridad y Protección Ciudadana (SSPC), con autonomía técnica y de operación, de conformidad con los artículos 2, fracción I, 45, 46, 55 y 56 fracción III del Reglamento Interior de la Secretaría de Seguridad y Protección Ciudadana (RISSPC) y, es sujeto obligado[1] en términos de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO).

Por ello, es responsable de proteger los datos personales que trate, garantizando los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, los deberes de seguridad y confidencialidad, y las obligaciones derivadas de la LGPDPPSO.

El presente documento constituye una Política Interna de Protección de Datos Personales del CENAPRED (Política), elaborado en observancia al principio de responsabilidad, el cual prevé que la o el responsable del tratamiento de los datos personales deberá implementar mecanismos para el cumplimiento de los principios, deberes y obligaciones establecidos en las disposiciones en materia de protección de datos personales, en cumplimiento a lo previsto por el artículo 29 de la mencionada Ley General y 47 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales)[2].

Estos mecanismos, prevé la ley, deben tener por objeto establecer los elementos y las actividades de dirección, operación y control de todos sus procesos que, en el ejercicio de funciones y atribuciones, impliquen un tratamiento de datos personales a efecto de proteger éstos de manera sistemática y continua.

Los responsables del tratamiento de los datos personales, para el caso en concreto el CENAPRED, no sólo debe tomar las medidas necesarias para cumplir con los principios, deberes y obligaciones antes señaladas, sino que además es deseable que realice un esfuerzo adicional para observar las mejores prácticas y estándares en la protección de datos personales, y para que rinda cuentas con relación al uso y cuidado de la información personal que esté en su posesión.

Para ello, existe la autorregulación, mediante la cual, de manera voluntaria, los responsables pueden adoptar un mecanismo que les ayude a mejorar el tratamiento y cuidado de los datos personales.

Bajo esta tesitura, con la instrumentación de esta Política, se pretende, facilitar a las personas servidoras públicas titulares de las Unidades Administrativas adscritas al CENAPRED a realizar un tratamiento de datos personales en estricto apego a los principios, deberes y obligaciones establecidos en la Ley General y demás disposiciones aplicables, lo cual permitirá garantizar la adecuada protección de los datos personales y el ejercicio de los derechos de Acceso, Rectificación, Cancelación, Oposición "ARC0" y Portabilidad al tratamiento de datos personales por parte de sus

[1] Sujeto obligado en términos de los artículos I y 3, fracción XXVIII de la Ley General, son sujetos obligados en el ámbito federal, estatal y municipal cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos Políticos, fideicomisos y fondos públicos, responsables de decidir el tratamiento de los datos personales

[2] Publicados en el Diario Oficial de la Federación el 26 de enero de 2018.

titulares.
Ahora bien, en atención a lo dispuesto por el artículo 57 del RISSPC[3] y de acuerdo con el Manual de Organización Específico del CENAPRED de fecha 15 de julio de 2021, dentro de las funciones de la Dirección de Servicios Técnicos (DST) se encuentra la de dirigir la Unidad de Transparencia del CENAPRED en la recepción y trámite de las solicitudes de acceso a la información, para cumplir con las obligaciones conforme a la normatividad aplicable, por ende es la unidad administrativa es la encargada de presidir el Comité de Transparencia del Centro Nacional.

Derivado de lo anterior, de conformidad con el Artículo 85, fracción VII de la LGPDPPSO, la DST será la responsable de asesorar a todas las Unidades Administrativas que integran el CENAPRED en materia de protección de datos personales.

[3] Artículo 57.- El Centro Nacional de Prevención de Desastres, para el ejercicio de sus funciones sustantivas de investigación, desarrollo de sistemas de información sobre riesgos, instrumentación, monitoreo, educación, capacitación, difusión, apoyo técnico, administrativo e interinstitucional, contará con las unidades administrativas subalternas que se determinen conforme a la estructura orgánica autorizada, cuyos titulares serán nombrados por el Secretario a propuesta del Director General del Centro Nacional de Prevención de Desastres. Las funciones y atribuciones de estas unidades administrativas subalternas se regirán por el Manual de Organización específico del Centro.

Política Interna de Protección de Datos Personales

PROPÓSITO

Garantizar el cumplimiento de los principios, deberes y obligaciones en materia de protección de datos personales, establecer mejores prácticas y estándares, así como elementos y actividades de dirección, operación y control en los procesos en que las Unidades Administrativas del CENAPRED, que en el ejercicio de sus funciones realicen algún tratamiento de datos personales.

ALCANCE

La presente Política es de observancia general para todas las personas servidoras públicas adscritas al CENAPRED involucradas en el tratamiento de datos personales.

La aplicación y cumplimiento de la presente Política, es obligatoria para las personas servidoras públicas Titulares de las Unidades Administrativas responsables de cualquier tratamiento de datos personales con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización, así como establecer las medidas necesarias que garanticen la seguridad de los datos personales que el ámbito de su competencia posean, recaben o transmitan, a fin de evitar su alteración, daño, destrucción o su uso, acceso o tratamiento no autorizado, pérdida y transmisión, debiendo asegurar su manejo para los propósitos para los cuales se hayan obtenido. Lo anterior de conformidad con lo establecido en los artículos 3, fracción I y XXXIII y 4 de la LGPDPPSO.

REFERENCIAS NORMATIVAS

- Constitución Política de los Estados Unidos Mexicanos, artículo 6°, Base A y segundo párrafo del artículo 16.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Reglamento Interior de la Secretaría de Seguridad y Protección Ciudadana.
- Manual de Organización Específico, Órgano Administrativo Desconcentrado, Centro Nacional de Prevención de Desastres.
- Lineamientos Generales de Protección de Datos Personales para el Sector Público.
- Lineamientos que establecen los parámetros, modalidades y procesamiento para la portabilidad de datos personales.
- Lineamientos de Operación y Funcionamiento del Comité de Transparencia del Centro Nacional de Prevención de Desastres.
- Guía para cumplir con los principios y deberes de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Política Interna de Protección de Datos Personales

GLOSARIO

En adición a los términos establecidos en el artículo 3 de la LGPDPPSO, para efectos de la presente Política, se entenderá por:

Capacitación.- Medida de seguridad para establecer las políticas y procedimientos de entrenamiento basado en roles y responsabilidades.

CENAPRED.- Centro Nacional de Prevención de Desastres.

Ciclo de vida.- De conformidad con el artículo 59 de los Lineamientos Generales, se refiere a las fases del tratamiento de los datos personales, consistentes en la obtención, almacenamiento, uso, divulgación, bloqueo y cancelación.

Comité de Transparencia.- Comité de Transparencia del CENAPRED, autoridad máxima en materia de datos personales.

Deberes.- A los deberes de confidencialidad y de seguridad contemplados en los artículos 31, 32, 33, 34, 35, 36 y 42 LGPDPPSO y 55 al 65 y 71 de los Lineamientos Generales.

DST.- A la Dirección de Servicios Técnicos y Unidad de Transparencia del CENAPRED.

Enlace de datos personales.- A las personas servidoras públicas designadas por las personas Titulares de las Unidades Administrativas del CENAPRED, a efecto de fungir como enlace ante el Comité de Transparencia y la DST, en las responsabilidades que susciten en materia de protección de datos personales.

Inventario de datos personales.- Identificación de las bases de datos de tratamiento de las Unidades Administrativas, por el cual, se documenta la información básica de cada tratamiento realizado, con independencia de su forma de almacenamiento, entre lo cual se incluye el ciclo de vida del dato personal.

Ley General.- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

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

MOE.- ·Al Manual de Organización Específico, Órgano Administrativo Desconcentrado, Centro Nacional de Prevención de Desastres.

Órgano Garante.- Al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Órgano Interno de Control.- Al Órgano Interno de Control en la Secretaría de Seguridad y Protección Ciudadana y en el CENAPRED.

Política Interna de Protección de Datos Personales

Política.- Política Interna de Protección de Datos Personales del CENAPRED.

Portabilidad de Datos Personales.- Prerrogativa de los titulares de datos personales que les permite, bajo las condiciones establecidas en la normatividad aplicable, recibir los datos personales que han proporcionado a un responsable del tratamiento en un formato estructurado, de uso común y lectura mecánica, y transmitirlos a otro responsable del tratamiento sin impedimentos.

Principios.- Los ocho principios bajo los cuales se rige el derecho a la protección de los datos personales, los cuales se traducen en obligaciones, que son: licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad.

Reglamento Interior.- Reglamento Interior de la Secretaría de Seguridad y Protección Ciudadana.

Sujeto Obligado Receptor.- Cualquier autoridad, dependencia, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, tribunales administrativos, fideicomisos y fondos públicos y partidos políticos del orden federal, estatal o municipal, que recibe directamente del CENAPRED los datos personales, en un formato estructurado y comúnmente utilizado, a petición de la persona titular.

Titular.- La persona física a quien corresponden o conciernen los datos personales sujetos a tratamiento y por tanto es quien se considera como sujeto de protección del derecho a la protección de datos personales.

Titular de la Unidad Administrativa.- Persona responsable del tratamiento de los datos personales en la unidad administrativa a su cargo de conformidad con el artículo 57 del Reglamento Interior.

Unidad Administrativa.- Las previstas en el numeral VI del Manual de Organización Específico del CENAPRED.

Política Interna de Protección de Datos Personales

CAPÍTULO I
Disposiciones Generales

Primera.- La presente Política es de observancia general para todo el personal del CENAPRED involucrado en el tratamiento de datos personales.

El Comité de Transparencia como autoridad máxima en la materia velará por el debido cumplimiento y aplicación de la misma.

Segunda.- La DST asesorará a las Unidades Administrativas en materia de protección de datos personales conforme a los principios, deberes y obligaciones establecidos en la Ley General, los Lineamientos Generales, la presente Política y demás normativa aplicable.

Tercera.- Para las actividades señaladas en la presente Política, será necesario contar con personas servidoras públicas que actúen como enlaces en materia de datos personales.

Las personas Titulares de las Unidades Administrativas designarán a una persona servidora pública como enlace en materia de protección de datos personales, para establecer un canal de comunicación efectivo entre la DST y las Unidades Administrativas del CENAPRED.

Cuarta.- Las personas Titulares de las Unidades Administrativas son los responsables del tratamiento de los datos personales en el ámbito de sus funciones; y, por lo tanto, tendrán la obligación de cumplir los principios, deberes y obligaciones establecidos en la Ley General, los Lineamientos Generales, la presente Política y demás normativa aplicable.

Quinta.- El Comité de Transparencia y/o la DST, conjunta o separadamente, podrán sugerir a las Unidades Administrativas que realicen o dejen de hacer ciertas acciones con el fin de prevenir algún incumplimiento a las disposiciones en materia de protección de datos personales.

Sexta.- El Comité de Transparencia y/o la DST cuando adviertan un hecho que pueda constituir una probable falta administrativa en materia de datos personales en términos de la normativa aplicable, darán vista al Órgano Interno de Control para su conocimiento.

Séptima.- La DST, se auxiliará de las personas servidoras públicas adscritas a la misma para el ejercicio de sus funciones previstas en la presente Política, así como del personal habilitado en materia de transparencia.

CAPÍTULO II
De los Principios de Protección de Datos Personales

Octava.- De conformidad con el artículo 16 de la Ley General en relación con el artículo 7 de los Lineamientos Generales, los principios de protección de datos personales, son las herramientas para garantizar la efectiva protección de los datos personales de sus titulares cuando son tratados; herramientas de uso obligatorio para interpretar y aplicar la Ley General y demás normativa aplicable y representar un límite al tratamiento de datos personales que se encuentran en posesión de sujetos

obligados normativa aplicable y representar un límite al tratamiento de datos personales que se encuentran en posesión de sujetos obligados.

Novena.- El derecho a la protección de datos personales se rige a través de ocho principios, que son, Licitud, Finalidad, Lealtad, Consentimiento, Calidad, Proporcionalidad, Información y Responsabilidad. Por lo tanto las personas Titulares de las Unidades Administrativas del CENAPRED responsables del tratamiento de datos personales deberán observar esos principios rectores de la protección de datos personales.

Décima.- Principio de Licitud. El tratamiento de datos personales por parte de las personas Titulares de las Unidades Administrativas del CENAPRED debe ser realizado de conformidad con las funciones y atribuciones o facultades que previamente se otorgan en la normativa aplicable que le confiera, en este sentido, no deben tratarse datos personales si no se sujetan a las facultades previamente conferidas.

Décima Primera.- Obligación vinculada al Principio de Licitud. Es una obligación de las personas Titulares de las Unidades Administrativas, identificar el marco normativo que en el ámbito de sus atribuciones se encuentra relacionado con el tratamiento de datos personales, el tipo de datos objeto de tratamiento y las finalidades para ello, los cuales deben ser tratados de manera lícita.

Décima Segunda.- Para acreditar el cumplimiento del principio de licitud, las personas Titulares de las Unidades Administrativas, deberán incluir en el aviso de privacidad integral y en el inventario de datos personales, el fundamento legal que les faculta tratar datos personales.

Décima Tercera.- Principio de Finalidad. Todo tratamiento de datos personales efectuado por las personas Titulares de las Unidades Administrativas tendrá que estar justificado por las finalidades concretas, explícitas, lícitas y legítimas. Para tal efecto, se entenderá que las finalidades son:

a) Concretas: Atender el tratamiento de los datos personales con los fines específicos o determinados para los que fueron recabados, sin que admitan errores, distintas interpretaciones o provoquen incertidumbre, dudas o confusión a su titular;
b) Explícitas: Señalar y dar a conocer de manera clara en el aviso de privacidad que corresponda las finalidades relativas al tratamiento de datos personales;
c) Lícitas: Las finalidades que justifiquen el tratamiento de los datos personales deben ser acordes con las atribuciones o facultades de la Unidad Administrativa conforme a la normatividad aplicable;
d) Legítimas: Cuando las finalidades que motivan el tratamiento de los datos personales se encuentran autorizadas por el consentimiento de su titular, salvo que se actualicen las excepciones previstas en la Ley General, en la presente Política y demás normativa aplicable.

La finalidad o finalidades del tratamiento de datos personales deberán ser determinadas, es decir, deberán especificar para qué objeto se tratarán los datos personales de manera clara, sin lugar a confusión y con objetividad.

Décima Cuarta.- Las obligaciones para su cumplimiento por parte de las personas Titulares de las Unidades Administrativas que traten datos personales, son las siguientes:

Política Interna de Protección de Datos Personales

I. Tratar los datos personales únicamente para la finalidad o finalidades que hayan sido informadas a su titular en el aviso de privacidad y, en su caso, consentidas;
II. Informar en el aviso de privacidad todas las finalidades para las cuales se tratarán los datos personales y redactarlas de forma tal que sean determinadas;
III. Identificar y distinguir en el aviso de privacidad entre las finalidades que dan origen al tratamiento de aquellas que son distintas a las que lo originaron, pero se consideran compatibles y/o análogas;
IV. Ofrecer a la o el titular de los datos personales un mecanismo para que pueda manifestar su negativa al tratamiento de sus datos personales para todas o algunas de las finalidades secundarias;
V. Tratar los datos personales para finalidades distintas que no resulten compatibles o análogas con aquéllas para las que se hubiese recabado de origen los datos personales y que hayan sido previstas en el aviso de privacidad, al menos que lo permita una ley o reglamento, o se obtenga el consentimiento de la o el titular de los datos.

Décima Quinta.- Para acreditar el debido cumplimiento a este principio por parte de las personas Titulares de las Unidades Administrativas, se deberá realizar lo siguiente:

I. Contar con un inventario en el que se observen las finalidades de cada tratamiento que realice en su unidad administrativa, verificar que estas sean específicas y/o determinadas y que sean acordes a sus atribuciones o facultades;
II. Vigilar que las personas servidoras públicas a su cargo, únicamente traten datos personales en términos de las finalidades informadas en el aviso de privacidad correspondiente;
III. Verificar que en los avisos de privacidad informen, todas las finalidades para las cuales se tratan los datos personales y que éstas sean descritas de manera clara;
IV. Informar a los y las titulares las finalidades sobre el tratamiento de sus datos personales;
V. Recabar el consentimiento de los y las titulares para el tratamiento de datos personales, cuando el mismo se requiera.

Décima Sexta.- Principio de Lealtad. Las personas Titulares de las Unidades Administrativas se abstendrán de obtener y tratar datos personales a través de medios engañosos o fraudulentos. Con este principio no se permite un tratamiento tramposo, deshonesto y no ético de los datos personales de los y las titulares.

Décima Séptima.- Las obligaciones para su cumplimiento por parte de las personas Titulares de las Unidades Administrativas que tratan datos personales, son las siguientes:

I. Verificar que los datos personales no se recaben con dolo, mala fe o negligencia;
II. Comprobar que el tratamiento de los datos personales no genere discriminación o un trato injusto o arbitrario contra sus titulares;
III. Evitar quebrantar la confianza de los y las titulares en relación con sus datos personales que serán tratados conforme a lo acordado;
IV. Informar todas las finalidades del tratamiento en el aviso de privacidad.

Política Interna de Protección de Datos Personales

Décima Octava.- Para acreditar el cumplimiento a este principio por parte de las personas Titulares de las Unidades Administrativas, se deberá realizar lo siguiente:

a) Contar con avisos de privacidad que cumplan con lo establecido en la Ley General, la presente Política y demás normativa aplicable;
b) Implementar instrumentos que permitan verificar que los tratamientos realizados no den lugar a discriminación, trato injusto o arbitrario en contra de la o el titular;
c) Constatar que el tratamiento de datos personales sólo se lleve a cabo para los fines informados en el aviso de privacidad.

Décima Novena.- Principio de Consentimiento. Previo al tratamiento de los datos personales, las personas Titulares de las Unidades Administrativas deberán obtener el consentimiento de las y los titulares de los datos personales de manera libre, específica, inequívoca e informada, salvo que no sea requerido, en virtud de las siguientes causales de excepción:

a) Cuando una ley así lo disponga, en cuyo caso, los supuestos de excepción deberán ser acordes con las bases, principios y disposiciones establecidos en la Ley General que, en ningún caso, podrán contravenirla;
b) Cuando las transferencias que se realicen entre el CENAPRED y otro sujeto responsable sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o acordes con la finalidad que motivó el tratamiento de los datos personales;
c) Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;
d) Para el reconocimiento o defensa de derechos de la persona titular ante autoridad competente;
e) Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el o la titular y el CENAPRED.
f) Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;
g) Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico o la prestación de asistencia sanitaria;
h) Cuando los datos personales figuren en fuentes de acceso público;
i) Cuando los datos personales se sometan a un procedimiento previo de disociación.
j) Cuando la o el titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley en la materia.

De conformidad con el artículo 21 de la Ley General, el consentimiento podrá manifestarse de forma expresa o tácita, expreso o por escrito de su titular para el tratamiento de datos personales.

Por regla general, el consentimiento tácito será válido para llevar a cabo el tratamiento de datos personales, salvo aquellos supuestos en los cuales la Ley General o alguna disposición aplicable exija su obtención de forma expresa y, en su caso, por escrito, particularmente, cuando se refiera a datos sensibles.

La actualización de alguno de los supuestos señalados en los incisos anteriores, no exime a las personas Titulares de las Unidades Administrativas responsables del tratamiento de datos personales

del cumplimiento de las demás obligaciones establecidas en la Ley General, en la presente Política y demás normativa aplicable.

Vigésima.- Las obligaciones relacionadas con el cumplimiento del principio de consentimiento por parte de las personas Titulares de las Unidades Administrativas que traten datos personales, son las siguientes:

I. Obtener el consentimiento de la o el titular, previo al tratamiento de los datos personales, salvo que se actualice alguno de los supuestos de excepción descritos en la política Décima Novena;
II. Recabar el consentimiento expreso y, en su caso, por escrito, a través de formatos claros y sencillos, acorde con el perfil de la o el titular, en los cuales se distingan los datos personales y finalidades del tratamiento que requieren de la manifestación de su voluntad;
III. Implementar medios sencillos y gratuitos para la obtención del consentimiento, independientemente de la modalidad en que se requiera;
IV. En su caso, habilitar en el aviso de privacidad casillas y/o espacios para que la o el titular exprese su consentimiento, respecto de cada una de las finalidades para las cuales son tratados sus datos personales.

Vigésima Primera.- Para acreditar el cumplimiento a este principio por parte de las personas Titulares de las Unidades Administrativas, se deberá realizar lo siguiente:

a) Identificar en el aviso de privacidad, aquellos datos personales y finalidades que requieren del consentimiento de su titular, para su tratamiento;
b) Mantener bajo su resguardo una copia del documento en el cual se haya manifestado el consentimiento de la o el titular para el tratamiento de sus datos, cuando éste proceda;
c) Documentar la puesta a disposición del aviso de privacidad a la o el titular, en aquellos casos en los cuales sea válidos el consentimiento tácito.

Vigésima Segunda.- Principio de Información. Las personas Titulares de las Unidades Administrativas del CENAPRED que traten datos personales, se encuentran obligadas a informar a las personas titulares, las características principales del tratamiento al que será sometida su información personal, lo que se materializa a través del aviso de privacidad. En ese sentido, se deberá elaborar y poner a disposición los avisos de privacidad integral y simplificado que correspondan al tratamiento que lleven a cabo, en los términos establecidos en la Ley General, en la presente Política y demás normativa aplicable, independientemente de que se requiera o no el consentimiento del o la titular.

Vigésima Tercera.- Las obligaciones para el cumplimiento del principio de Información por parte de las personas Titulares de las Unidades Administrativas que traten datos personales, son las siguientes:

I. Redactar y elaborar el aviso de privacidad en sus dos modalidades: integral y simplificado, con las características principales del tratamiento al que serán sometidos los datos personales de su titular, estructurado de manera clara y sencilla que facilite su entendimiento y con los elementos establecidos por la Ley General y los Lineamientos Generales y tomando en consideración los Criterios de elaboración del CENAPRED emitidos para tal efecto.

Política Interna de Protección de Datos Personales

II. Poner a disposición de las y los titulares el aviso de privacidad en los términos que fije la Ley General y los Lineamientos Generales, aunque no se requiera el consentimiento para el tratamiento de sus datos personales;
III. Difundir, poner a disposición o reproducir el aviso de privacidad en formatos físicos y electrónicos, ópticos, sonoros, visuales o a través de cualquier otra tecnología que permita su eficaz comunicación y permitan la accesibilidad para grupos vulnerables;
IV. Comunicar en el aviso de privacidad simplificado e integral, la información relativa en caso de haber transferencias;

Vigésima Cuarta.- Las personas Titulares de las Unidades Administrativas preverán excepcionalmente o cuando resulte imposible dar a conocer a las y los titulares el aviso de privacidad de manera directa o ello exija esfuerzos desproporcionados, instrumentar algún mecanismo o medidas para la comunicación masiva del aviso de privacidad.

Se considerará que existe una imposibilidad para dar a conocer el aviso de privacidad de forma directa, cuando el responsable no cuente con los datos personales necesarios que le permitan tener contacto directo con los titulares, ya sea porque no existen en sus archivos, registros o bases de datos, o bien, porque los mismos se encuentran desactualizados, incorrectos, incompletos o inexactos.

Vigésima Quinta.- Para acreditar el cumplimiento del principio de información, se deberá realizar lo siguiente:

a) Contar con los avisos de privacidad integral y simplificado por cada proceso de tratamiento de datos personales que se lleve a cabo;
b) Implementar un procedimiento o medio para la puesta de disposición del aviso de privacidad;
c) Realizar las gestiones para que los avisos de privacidad, en su modalidad simplificada e integral, sean plasmados en un lugar visible que permita la consulta del o la titular, conforme a lo establecido en las obligaciones señaladas en la política vigésima tercera;
d) Incluir en el inventario los lugares y medios en los que se difunden y colocan los avisos de privacidad;
e) Documentar la comunicación realizada del aviso de privacidad a terceras personas a las que se transfieran los datos personales.

Vigésima Sexta.- Principio de Proporcionalidad. Las personas Titulares de las Unidades Administrativas del CENAPRED, recabarán aquellos datos personales que resulten necesarios, adecuados y relevantes 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.

Vigésima Séptima.- Las obligaciones para su cumplimiento por parte de las Unidades Administrativas que traten datos personales, son las siguientes:

I. Recabar y tratar sólo aquellos datos personales necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron y, en su caso, privilegiar la utilización de datos generados por el propio CENAPRED, para que el tratamiento de datos personales de la o el

titular no sea excesivo, como por ejemplo usar el número de empleado en lugar de la CURP o el RFC;

II. Realizar esfuerzos razonables para limitar los datos personales tratados al mínimo necesario, considerando las finalidades que motivan su tratamiento;
III. Limitar al mínimo posible el periodo de tratamiento de datos personales;
IV. Verificar si los datos personales que serán requeridos por la persona Titular de la Unidad Administrativa para su tratamiento, ya son tratados por otra persona Titular de una Unidad Administrativa diversa a la anterior.

Vigésima Octava.- Para acreditar el debido cumplimiento a este principio por parte de las personas Titulares de las Unidades Administrativas, deberá realizar lo siguiente:

a) Analizar y revisar que en su área se soliciten sólo aquellos datos personales que resultan indispensables para cumplir con las finalidades de que se trate;
b) Establecer con precisión los datos personales que deberán tratarse para cumplir con la finalidad, cuando una normativa establezca su obtención, sólo se deberán solicitar dichos datos;
c) Promover prácticas que minimicen la obtención de datos personales.

Vigésima Novena.- Principio de Calidad. Las personas Titulares de las Unidades Administrativas del CENAPRED, deberán mantener los datos personales conforme a la finalidad o finalidades para las que se hayan recabado y adoptar las medidas necesarias para mantenerlos exactos, correctos, completos y actualizados a fin de que no se altere su veracidad. Se puntualiza que estas características de los datos personales tienen el siguiente alcance:

- Exactos: se considera que los datos personales son exactos cuando reflejan la realidad de la situación de su titular, es decir, son verdaderos o fieles;
- Correctos: son correctos cuando no presentan errores que pudieran afectar su veracidad;
- Completos: cuando la integridad de los datos personales permite el cumplimiento de las finalidades que motivaron su tratamiento y de las atribuciones del o la responsable;
- Actualizados: cuando los datos personales responden fielmente a la situación actual de su titular.

Se presume que se cumple con la calidad en los datos personales cuando éstos son proporcionados directamente por su titular y hasta que éste no manifieste y acredite lo contrario.

Trigésima.- Las personas Titulares de las Unidades Administrativas responsables deberán adoptar las medidas para garantizar que los datos personales cumplan con las características del Principio de Calidad, a fin de que no se altere la veracidad de la información, ni que ello tenga como consecuencia que la o el titular se vea afectado por dicha situación.

En el supuesto de que los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones aplicables, serán suprimidos, previo bloqueo en su caso, y una vez que concluya el plazo de conservación.

Política Interna de Protección de Datos Personales

Trigésima Primera.- Las obligaciones vinculadas en el cumplimiento del principio de calidad, por parte de las personas Titulares de las Unidades Administrativas que traten datos personales, son las siguientes:

I. Adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales, principalmente cuando se obtuvieron de manera indirecta de la o el titular;
II. Establecer plazos de conservación de la información, conforme a las disposiciones legales aplicables en materia archivística;
III. Establecer y documentar los procedimientos para la conservación, bloqueo y supresión de los datos personales cumpliendo los plazos previstos para ello, o bien, en atención a una solicitud de ejercicio del derecho de cancelación.

Trigésima Segunda.- Para acreditar el debido cumplimiento de este principio por parte de las Unidades Administrativas, se deberá realizar lo siguiente:

a) Generar una relación de todas las bases de datos con que cuentan y el tipo de información personal tratada en cada una de ellas que, en su caso, permita vincularlas;
b) Documentar las actualizaciones y supresiones realizadas;
c) Contar con los procedimientos para la conservación, bloqueo y supresión de los datos personales.

Trigésima Tercera.- Principio de Responsabilidad. Conforme al principio de responsabilidad, las personas Titulares de las Unidades Administrativas velarán por el cumplimiento del resto de los principios, adoptarán medidas necesarias como estándares y mejores prácticas para su aplicación y demostrarán ante las y los titulares y al Órgano garante que cumple con sus obligaciones en torno a la protección de datos personales.

Asimismo, el Principio de Responsabilidad también es conocido por el principio de rendición de cuentas, ya que como bien se dijo en el párrafo anterior, establece la obligación de velar por el cumplimiento del resto de los principios, así como los deberes que establece la normativa aplicable para dar cuenta a los y las titulares y la autoridad de que se cumple con las obligaciones de protección de datos personales. Por ello, la DST será la encargada de pedir cuentas a las Unidades Administrativas del CENAPRED en materia de protección de datos personales.

Trigésima Cuarta.- Las obligaciones para el cumplimiento del principio de Responsabilidad por parte de las personas Titulares de las Unidades Administrativas que traten datos personales, son las siguientes:

I. Participar en los programas de capacitación y actualización en materia de protección de datos personales;
II. Establecer procedimientos para recibir y responder dudas y quejas de los y las titulares;
III. Diseñar o modificar las políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología con que cuente y que implique el tratamiento de datos personales, para que desde el inicio cumplan por diseño con

las obligaciones previstas en la Ley General, los Lineamientos Generales, la presente Política y demás normativa aplicable, previa opinión del Comité de Transparencia;

IV. Cumplir con los principios y deberes que establece la Ley General, los Lineamientos Generales, la presente Política y demás normativa aplicable.

Trigésima Quinta.- Las obligaciones para el cumplimiento del Principio de Responsabilidad, por parte de la Unidad de Transparencia:

I. Recopilar de las Unidades Administrativas que traten datos personales, los insumos necesarios para elaborar un Programa de Protección de Datos Personales que provea los elementos y actividades de dirección, operación y control de los procesos en el CENAPRED, para proteger de manera sistemática y continua de los datos personales;
II. Diseñar e implementar a través del enlace de capacitación del CENAPRED, los programas de capacitación y actualización que tengan por obligación capacitar al personal involucrado en el tratamiento de datos personales;
III. Coordinar a las Unidades Administrativas del CENAPRED para que recopilen los datos personales que traten, así como los insumos necesarios para que las áreas correspondientes, elaboren el Documento de Seguridad que contemple las medidas de carácter administrativo, técnico, físico o cualquier otra;
IV. Revisar el cumplimiento de los procedimientos para recibir y responder dudas y quejas de las y los titulares.

Trigésima Sexta.- Para acreditar el debido cumplimiento al Principio de Responsabilidad por parte de las Unidades Administrativas, se deberá realizar lo siguiente:

I. Contar con las constancias de capacitación en materia de protección de datos personales;
II. Llevar un registro de las dudas y quejas de los y las titulares de datos personales;
III. Documentar la comunicación relacionada con el diseño o modificación de las políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología con que cuente y que implique el tratamiento de datos personales;
IV. Documentar la comunicación relacionada con el cumplimiento de los principios y deberes que establece la Ley General, los Lineamientos Generales, la presente Política y demás normativa aplicable.

Trigésima Séptima.- Para acreditar el debido cumplimiento del Principio de Responsabilidad por parte de la Unidad de Transparencia:

I. Coordinar a través del enlace de capacitación del CENAPRED la implementación del Programa en materia de Protección de Datos Personales;
II. Acreditar la capacitación con las listas de asistencia a los cursos en materia de protección de datos personales que al efecto proporcione el enlace de capacitación del CENAPRED;
III. Realizar en su caso, la actualización del Programa de Protección de Datos Personales y revisar el Documento de Seguridad;
IV. Evidenciar del cumplimiento de los procedimientos para recibir y responder dudas y quejas de las y los titulares en caso de que existan;

V. Observar el cumplimiento del procedimiento para el tratamiento de datos personales en políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología de diseño o modificación que cumplan con las obligaciones previstas en la Ley General, los Lineamientos Generales, la presente Política y demás normativa aplicable.
VI. Lineamientos Generales, la presente Política y demás normativa aplicable;
VII. Guardar evidencia de las acciones para asegurar y acreditar el cumplimiento de los principios y deberes que establece la Ley General, los Lineamientos Generales, la presente Política y demás normativa aplicable.

CAPÍTULO III
De los Deberes para la Protección de Datos Personales

Trigésima Octava.- La protección de los datos personales, prevé dos deberes, el de confidencialidad y el de seguridad.

La importancia de estos deberes es proteger los datos personales de cualquier amenaza de riesgo con potencial para provocarles un daño o perjuicio, como el robo, extravío o copia no autorizada, pérdida o destrucción no autorizada, uso o acceso no autorizado, daño, alteración o modificación no autorizado.

Con estos deberes se garantiza la Confidencialidad, Integridad y Disponibilidad. Entendiéndose por éstos:

- **Confidencialidad**: Es la obligación del o la responsable de guardar secrecía de los datos personales, para que no estén a disposición o sean revelados a terceras personas.
- **Integridad**: Es la obligación del o la responsable de salvaguardar la exactitud y completitud de los datos personales.
- **Disponibilidad**: Es la obligación del o la responsable de que los datos personales, sean accesibles y utilizables cuando se requiera.

Trigésima Novena.- Las personas Titulares de las Unidades Administrativas responsables del tratamiento de datos personales, con independencia del tipo de soporte en el que se encuentren o el tipo de tratamiento que se realice, deberán establecer las medidas de seguridad de carácter administrativo, físico y técnico para la protección de datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, y así garantizar su confidencialidad, integridad y disponibilidad; por lo tanto deberán observar los deberes de seguridad, contemplados en los artículos 31, 32, 33, 34, 35 y 36 Ley General y artículos 55 al 65 Lineamientos Generales; y de Confidencialidad dispuesto en los artículos 42 y 71 de la Ley General y Lineamientos Generales, respectivamente.

Cuadragésima.- Deber de Seguridad. Las personas Titulares de las Unidades Administrativas del CENAPRED, adoptarán e instrumentarán las medidas físicas, técnicas y administrativas a través de las cuales garantice la protección de datos personales.

Cuadragésima Primera.- Las obligaciones vinculadas con el cumplimiento del deber de seguridad por

parte de las personas Titulares de las Unidades Administrativas que traten datos personales serán:

I. Generar e implementar políticas de gestión, en las cuales se considere el tipo de datos personales recabados, el tratamiento que se les dará y el ciclo de vida, es decir, su obtención, uso y posterior supresión;
II. Designar a las personas servidoras públicas que podrán intervenir en el tratamiento de los datos personales y definir las funciones y obligaciones que tendrán;
III. Realizar un análisis de riesgo de los datos personales tratados, así como de los sistemas físicos y/o electrónicos en los cuales se desarrolle dicho tratamiento;
IV. Realizar un análisis de brecha y desarrollar acciones de prevención y mitigación de amenazas o vulneraciones de datos personales;
V. Monitorear y revisar las medidas de seguridad adoptadas para garantizar la protección de datos;
VI. Incentivar la capacitación de las personas servidoras públicas involucradas en el tratamiento de datos personales, conforme al nivel de responsabilidad que tengan asignado.

Cuadragésima Segunda.- Para acreditar el cumplimiento de este deber por parte de las personas Titulares de las Unidades Administrativas, se deberá realizar lo siguiente:

a) Contar con un inventario de las bases de datos personales;
b) Describir los roles y las responsabilidades específicas de las personas servidoras públicas relacionadas con el tratamiento de datos personales;
c) Implementar mecanismos y/o políticas para la protección de datos y guardar evidencia de ello;
d) Llevar una bitácora en la cual se asiente cualquier amenaza o vulneración de datos personales suscitada, así como de las acciones realizadas para su mitigación;
e) Instrumentar las medidas de seguridad físicas, técnicas y administrativas adoptadas para garantizar el tratamiento de los datos recabados, así como las acciones de monitoreo, análisis y revisión a implementar; a fin de mantenerlas actualizadas y, en su caso, detectar áreas de oportunidad para su desarrollo y ejecución;
f) Tener la evidencia documental de los cursos, talleres, seminarios o similares en los que haya participado el personal adscrito a la Unidad Administrativa y se encuentren relacionados con la materia de protección de datos personales.

Cuadragésima Tercera.- Deber de Confidencialidad. Las personas Titulares de las Unidades Administrativas del CENAPRED que traten datos personales deberán establecer controles o mecanismos de observancia obligatoria para las personas servidoras públicas que intervengan en cualquier fase del tratamiento, mantengan en secreto la información, así como evitar que los datos personales sean revelados a personas no autorizadas y prevenir la divulgación no autorizada de los mismos, obligación que subsistirá aún después de finalizar sus relaciones con el mismo.

Por lo anterior, todas las personas servidoras publicas adscritas al CENAPRED que traten datos personales, tendrán la obligación de guardar secreto respecto de los datos personales, para evitar causar un daño a su titular. De no ser así, un tercero no autorizado podría tener acceso a determinada información y hacer mal uso de esta.

Política Interna de Protección de Datos Personales

Cuadragésima Cuarta.- Las obligaciones vinculadas para su cumplimiento por parte de las personas Titulares de las Unidades Administrativas que traten datos personales son:

I. Prever controles mediante los cuales se garantice la confidencialidad de los datos personales que son tratados;
II. Establecer cláusulas en los contratos para que los sujetos obligados del ámbito público o privado a los cuales les sean transferidos o remitidos datos personales se obliguen a la confidencialidad de éstos durante y posterior a la vigencia del instrumento jurídico;
III. Implementar campañas de sensibilización para las personas servidoras públicas, sobre la importancia de la confidencialidad de los datos personales;
IV. Proponer la implementación de mejores prácticas al interior del CENAPRED para garantizar la secrecía de los datos personales.

Cuadragésima Quinta.- Para acreditar el cumplimiento a este deber por parte de las personas Titulares de las Unidades Administrativas, se deberá realizar lo siguiente:

a) Incluir en el Documento de Seguridad, los controles y las medidas de seguridad implementadas para garantizar la secrecía de los datos personales;
b) Generar evidencia de los controles implementados para garantizar la confidencialidad de los datos;
c) En su caso, contar con los contratos en los cuales se establezcan las cláusulas de confidencialidad de datos, respecto de transferencias o remisiones;
d) Tener la evidencia documental de los cursos, talleres, seminarios o similares en los que haya participado el personal adscrito a las Unidades Administrativas y se encuentren relacionados con la materia de protección de datos personales;
e) Documentar la implementación de mejores prácticas que garanticen la confidencialidad de los datos tratados.

CAPÍTULO IV
Documentos para la Protección de Datos Personales

Cuadragésima Sexta.- Para la Protección de Datos Personales, el CENAPRED contará con los siguientes documentos:

- **Documento de Seguridad:** Documento elaborado por cada una de las Unidades Administrativas del CENAPRED, cuyo propósito es establecer las medidas administrativas, físicas y técnicas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales.
- **Programa de Protección de Datos Personales**: Documento de planeación que tiene por objeto establecer elementos y actividades de dirección, operación y control de los procesos del CENAPRED, para proteger de manera sistemática y continúa los datos personales en posesión de éste.
- **Aviso de Privacidad**: Documento generado por las Unidades Administrativas del CENAPRED, para dar a conocer a las y los titulares los datos personales que son recabados y las finalidades de su tratamiento.
- **Programa de Capacitación**: Documento en el cual se prevén actividades de capacitación y

actualización para todas las personas servidoras públicas adscritas al CENAPRED, considerando sus roles y responsabilidades asignadas para el tratamiento de datos personales.

Cuadragésima Séptima.- El CENAPRED deberá contar con los Documentos de Seguridad correspondientes, como parte de los mecanismos implementados para asegurar el cumplimiento del deber de seguridad, cuyo objeto es describir y dar cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas, para la protección de datos personales que permitan protegerlos contra daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado, así como para garantizar la confidencialidad, integridad y disponibilidad de los datos personales.

El Documento de Seguridad deberá de ser aprobado por el Comité de Transparencia como máxima autoridad en materia de datos personales.

Cuadragésima Octava.- El Documento de Seguridad deberá contener como mínimo, lo siguiente:

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 anual de capacitación.

Cuadragésima Novena.- En las actualizaciones que se realicen al Documento de Seguridad deberán participar las personas Titulares de las Unidades Administrativas, a través de sus enlaces en materia de datos personales, quienes en todo momento observarán los principios, deberes y obligaciones a los que se refieren la Ley General, los Lineamientos Generales, la presente Política y demás normativa aplicable.

De conformidad con lo dispuesto en la Ley General, el Documento de Seguridad se actualizará en los supuestos siguientes:

I. Se produzcan modificaciones sustanciales al tratamiento de los datos personales que deriven en un cambio de nivel de riesgo;
II. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión con el que se cuente;
III. Derivado de un proceso de mejora para mitigar el impacto de vulneración a la seguridad ocurrida;
IV. Con motivo de la implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

Con independencia de los supuestos anteriores, el Documento de Seguridad podrá ser actualizado cada tres años.

Quincuagésima.- Cuando alguna de las personas Titulares de las Unidades Administrativas se

encuentre en algunos de los supuestos del artículo anterior, la o el enlace presentará por escrito a la DST las actualizaciones conducentes y está lo someterá al Comité de Transparencia para resolver lo conducente.

Quincuagésima Primera.- En términos de lo previsto en la Ley General, se considera como vulneraciones de seguridad, en cualquier fase del tratamiento de datos, al menos, las siguientes:

a) La pérdida o destrucción no autorizada;
b) El robo, extravío o copia no autorizada;
c) El uso, acceso o tratamiento no autorizado;
d) El daño, la alteración o modificación no autorizada.

Quincuagésima Segunda.- Las personas Titulares de las Unidades Administrativas deberán llevar una bitácora de las vulneraciones a la seguridad en las que se describa ésta, la fecha en la que ocurrió, el motivo de ésta y las acciones correctivas implementadas de forma inmediata y definitiva.

Quincuagésima Tercera.- Cuando las vulneraciones afecten de forma significativa los derechos patrimoniales o morales de las o los titulares de los datos personales, las personas Titulares de las Unidades Administrativas involucradas, deberán generar un informe detallado que contenga al menos lo siguiente:

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 personas titulares afectadas;
VI. Los sistemas de tratamiento y datos personales comprometidos;
VII. Las acciones correctivas realizadas de forma inmediata;
VIII. La descripción de las posibles consecuencias de la vulneración de seguridad ocurrida;
IX. Las recomendaciones dirigidas a las y los titulares;
X. El medio puesto a disposición del o la titular para que pueda obtener mayor información sobre la vulneración y cómo proteger sus datos personales;
XI. El nombre completo de la o las personas designadas para proporcionar mayor información al Órgano garante, en caso de requerirse;
XII. Cualquier otra información y documentación que considere conveniente hacer del conocimiento del Órgano garante.

Para efectos del presente numeral, se entenderá que se afectan los derechos patrimoniales de la o el titular, cuando la vulneración esté relacionada, de manera enunciativa más no limitativa, con sus bienes, información fiscal, historial crediticio, ingresos o egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados u otros similares.

De la misma manera, se entenderá que se afectan los derechos morales del o la titular, cuando la vulneración esté relacionada de manera enunciativa más no limitativa, con sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, aspecto físico o menoscabe ilegalmente la libertad, integridad física o psíquica de la titular de los datos.

Política Interna de Protección de Datos Personales

Quincuagésima Cuarta.- Las personas Titulares de las Unidades Administrativas tendrán la obligación de notificar a la(s) persona(s) titular(es) afectada(s) la información descrita en lo incisos anteriores, a través del medio que se establezca para ese fin, marcando copia de conocimiento a la UT.

En aquellos casos en los cuales no sea posible notificar directamente a la(s) personas (s) titular(es) afectada(s) sobre el informe a que hace referencia la presente Política o ello implique esfuerzos desproporcionados, se instrumentarán medidas compensatorias de comunicación para tal efecto, como son: la publicación en el periódico oficial, aviso en la página oficial de Internet, sitios de internet, plataformas, tarjetas o cápsulas informativas u otro similar.

Con independencia de lo anterior la persona Titular de la Unidad Administrativa, deberá sujetarse a lo señalado en el artículo 37 de la Ley General, que establece que, en caso de que ocurra una vulneración a la seguridad, el responsable deberá analizar las causas por las cuales se presentó e implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales si fuese el caso a efecto de evitar que la vulneración se repita.

Quincuagésima Quinta.- El informe al que se refiere el numeral 53° de la presente Política, se deberá remitir a la DST en un plazo no mayor de cuarenta y ocho horas hábiles posteriores a que se haya confirmado la vulneración de seguridad, para que ésta la haga del conocimiento al Órgano Garante en tiempo y forma, de conformidad con la Ley General, los Lineamientos Generales y demás normativa aplicable.

Quincuagésima Sexta.- En términos de lo previsto en el numeral anterior, la DST deberá informar al Comité de Transparencia de lo ocurrido en torno a la vulneración de seguridad de datos personales.

El Comité de Transparencia podrá determinar la implementación de acciones adicionales a las realizadas por las personas Titulares de las Unidades Administrativas para evitar futuras vulneraciones y reforzar las medidas de seguridad existentes.

El Comité de Transparencia podrá auxiliarse de la asesoría, orientación o apoyo de las personas Titulares de las Unidades Administrativas, en asuntos de su especialidad, con la finalidad de garantizar la efectiva protección de los datos personales.

Para llevar acabo lo anterior, el Comité de Transparencia se apoyará de la Unidad de Transparencia para llevar a cabo dichas gestiones ante las personas Titulares de las Unidades de Administrativas.

Quincuagésima Séptima.- El CENAPRED deberá contar con un Programa de Protección de Datos Personales aprobado por el Comité de Transparencia, cuyo objetivo serán los siguientes:

I. Proveer el marco de trabajo necesario para la protección de los datos personales en posesión del CENAPRED;
II. Cumplir con los principios, deberes y obligaciones de la Ley General, la presente Política y la normatividad que derive de los mismos;
III. Establecer los elementos y las 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;

IV. Promover la adopción de mejores prácticas en la protección de datos personales.

Quincuagésima Octava.- El Programa de Protección de Datos Personales deberá estar actualizado, sin demerito de que podrá ser sometido a su revisión o reajuste por parte del Comité de Transparencia, de conformidad con las facultades y atribuciones que le establece la normativa aplicable, en caso de estimarse necesario.

Quincuagésima Novena.- La DST tendrá las siguientes funciones en relación al Programa de Protección de Datos Personales:

I. Elaborar y coordinar el Programa en conjunto con las Unidades Administrativas que estime necesario involucrar o consultar;
II. Proponer cambios y mejoras al Programa, a partir de la experiencia de su implementación;
III. Dar a conocer el Programa al interior del sujeto obligado;
IV. Coordinar la implementación del Programa en las Unidades Administrativas;
V. Asesorar a las Unidades Administrativas en la implementación del Programa, con el apoyo de las áreas técnicas que estime pertinente;
VI. Las demás que de manera expresa señalen el propio Programa.

Sexagésima.- Como parte de las acciones para cumplir con el principio de información, en el CENAPRED se contará con los avisos de privacidad integral y su correlativo aviso de privacidad simplificado, para el tratamiento de datos personales.

Excepcionalmente, cuando dos o más tratamientos de datos personales, atiendan una misma finalidad o función, se podrá contar con un mismo aviso de privacidad, en sus dos modalidades, siempre y cuando sea posible expresar con precisión y claridad las finalidades del tratamiento de datos personales, de tal suerte que no dé lugar a incertidumbre o ambigüedad a sus titulares.

Sexagésima Primera.- Los formatos para la elaboración de los avisos de privacidad integral y simplificado serán acordes con los elementos que establecen en la Ley General, los Lineamientos Generales y demás normatividad que resulte aplicable.

Sexagésima Segunda.- En la integración y elaboración de los avisos de privacidad, las Unidades Administrativas preverán un diseño que facilite su entendimiento por parte de las y los titulares de los datos. La DST podrá elaborar propuestas de formatos que faciliten su integración o actualización, manteniendo la homogeneidad de los elementos.

En todo momento, los Titulares de las Unidades Administrativas, deberán asegurarse que los avisos de privacidad se encuentren actualizados.

Sexagésima Tercera.- Las personas Titulares de las Unidades Administrativas se asegurarán de que la información asentada en los avisos de privacidad se encuentre redactada en un lenguaje ciudadano, sencillo, claro y comprensible, considerando en todo momento el perfil de la o el titular al cual vaya dirigido, por lo que se abstendrán de:

I. Usar frases inexactas, ambiguas o vagas;
II. Incluir textos que induzcan a los y las titulares a elegir una opción en específico;
III. Marcar previamente casillas, en caso de que éstas se incluyan, para que los y las titulares otorguen su consentimiento, o bien, incluir declaraciones orientadas a afirmar que los y las titulares ha consentido el tratamiento de sus datos personales sin manifestación alguna de su parte;
IV. Remitir a textos o documentos que no estén disponibles para las y los titulares.

Sexagésima Cuarta.- El CENAPRED contará con un Programa de Capacitación y Actualización en materia de Protección de Datos Personales, como uno de los mecanismos a través de los cuales se cumple con el principio de responsabilidad, el cual considerará los niveles de capacitación atendiendo los roles y las responsabilidades de las personas servidoras públicas que tratan datos personales.

Sexagésima Quinta.- El Comité de Transparencia será el órgano encargado de aprobar el Programa de Capacitación y Actualización en la materia, con base en la propuesta que sea presentada por el enlace de capacitación del CENAPRED, en la cual se consideren las necesidades de capacitación de las Unidades Administrativas.

Sexagésima Sexta.- La DST coordinará y dará seguimiento a los programas de capacitación continua y especializada en la materia de protección de datos personales a través del enlace de capacitación del CENAPRED.

CAPÍTULO V
Ejercicio de los Derechos ARCO y la Portabilidad de los Datos Personales

Sexagésima Séptima.- Para efectos de la presente Política, los Derechos ARCO son aquellos derechos que tiene el o la titular de los datos personales, para solicitar el Acceso, Rectificación, Cancelación y Oposición sobre el tratamiento de sus datos.

- **Acceso**: Derecho del o la titular para acceder a sus datos personales y conocer la información relacionada con las condiciones y generalidades del tratamiento.
- **Rectificación**: Derecho del o la titular para solicitar la corrección de sus datos personales, cuando éstos resulten inexactos, incompletos o no se encuentren actualizados.
- **Cancelación:** Derecho del o la titular para solicitar que sus datos personales sean bloqueados y ulteriormente suprimidos de los archivos, registros, expedientes y sistemas.
- **Oposición:** Derecho del o la titular para solicitar que se abstengan de solicitar información personal para ciertos fines o de requerir que se concluya el uso a fin de evitar un daño.

Sexagésima Octava.- La DST será la responsable de turnar las solicitudes de ejercicio de derechos ARCO que sean presentadas en el CENAPRED a aquellas Unidades Administrativas que conforme a sus atribuciones, competencias o funciones puedan o deban poseer los datos personales, para que se pronuncien y den atención en los plazos y términos establecidos para la atención de Solicitudes de Acceso a la Información y de Solicitudes para el Ejercicio de los Derechos ARCO.

Política Interna de Protección de Datos Personales

Sexagésima Novena.- Cuando los datos personales se encuentren en un formato estructurado y comúnmente utilizado podrá proceder la portabilidad de los datos personales.

La Portabilidad de los datos personales, tiene por objeto que la o el titular solicite, lo siguiente:

I. Una copia de sus datos personales que hubiere facilitado directamente al CENAPRED una Unidad Administrativa, en un formato estructurado comúnmente utilizado, que le permita seguir utilizándolos y, en su caso, entregarlos a otro sujeto obligado para su reutilización y aprovechamiento en un nuevo tratamiento;
II. La transmisión de sus datos personales a un sujeto obligado receptor, siempre y cuando sea técnicamente posible, la o el titular hubiere facilitado directamente sus datos personales al CENAPRED y el tratamiento de éstos se base en su consentimiento o en la suscripción de un contrato.

CAPÍTULO VI
De las Remisiones y Transferencias de los Datos Personales

Septuagésima.- Se le conoce como remisión, a toda comunicación de datos personales realizada por la persona Titular de la Unidad Administrativa y la o el encargado dentro y fuera del territorio mexicano.

La figura de la o el encargado, es una persona prestadora de servicios que trata datos personales a nombre de la persona Titular de la Unidad Administrativa responsable de los datos personales.

La o el encargado, tiene las siguientes características: puede ser una persona física o jurídica, de ámbito público o privado, ajeno al CENAPRED, puede ser una sola persona o de manera conjunta con otras personas, no tiene poder de decisión sobre el alcance y contenido del tratamiento de los datos personales y debe delimitar sus actuaciones a lo que diga la persona Titular de la Unidad Administrativa responsable de los datos personales.

Septuagésima Primera.- La transferencia es toda comunicación de datos personales, dentro o fuera del territorio nacional, a persona distinta de la o el titular, de la persona Titular de la Unidad Administrativa o la o el encargado.

Toda transferencia de datos personales se encontrará sujeta al consentimiento de su titular. Para tal efecto, a través del aviso de privacidad correspondiente informarán al o la titular de los datos personales, las finalidades de la transferencia, así como el tercero receptor.

No se requerirá el consentimiento de la o el titular para llevar a cabo la transferencia de sus datos personales, en los casos previstos en los artículos 22, 66 y 70 de la Ley General.

CAPÍTULO VII
Supervisión en materia de Protección de Datos Personales

Septuagésima Segunda.- Para el debido cumplimiento de los principios, deberes y obligaciones que establecen la Ley General, los Lineamientos Generales y la normativa aplicable en materia de

Política Interna de Protección de Datos Personales

protección de datos personales, el Comité de Transparencia a través de la DST supervisará a las Unidades Administrativas para garantizar el derecho a la protección de datos personales en el CENAPRED de conformidad con lo dispuesto en el artículo 84 fracción I de la Ley General.

Septuagésima Tercera.- La supervisión en materia de protección de datos personales se sustanciará mediante requerimientos de información sobre el tratamiento de datos personales, así como de sugerencias a las Unidades Administrativas para prevenir algún incumplimiento a las disposiciones en materia de protección de datos personales.

TRANSITORIOS

PRIMERO.- La presente Política entrará en vigor a partir de su aprobación por el Comité de Transparencia del Centro Nacional de Prevención de Desastres.

SEGUNDO.- Notifíquese la presente Política a las personas Titulares de las Unidades Administrativas a través de la Unidad de Transparencia del CENAPRED, difúndase al interior del CENAPRED y publíquese en el sitio oficial de Internet del CENAPRED.

TERCERO.- La Unidad de Transparencia deberá elaborar y coordinar en conjunto con las Unidades Administrativas el Programa de Protección de Datos Personales y ser aprobado por el Comité de Transparencia del CENAPRED.

Política Interna de Protección de Datos Personales

APROBACIÓN

La presente Política Interna de Protección de Datos Personales del Centro Nacional de Prevención de Desastres fue aprobada por el Comité de Transparencia en su Segunda Sesión Ordinaria del ejercicio fiscal 2022, celebrada el 06 de abril de 2022, al ser la autoridad máxima en materia de protección de datos personales de conformidad a los artículos 30, fracción II, 83, 84, fracción I y 87 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, artículo 47 de los Lineamientos Generales de Protección de Datos Personales y el artículo 7 de los Lineamientos de Operación y Funcionamiento del Comité de Transparencia del Centro Nacional de Prevención de Desastres.

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.