# Política Interna de Protección de Datos Personales en posesión de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros

# 2024

# Introducción

El presente documento, se elaboró en cumplimiento de lo previsto en el artículo 30, fracción II, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), normatividad que manifiesta la creación de políticas de protección de datos personales exigibles al interior del responsable de los datos, para dar cumplimiento al principio de responsabilidad establecido por la misma Ley, así como lo establecido por el artículo 47 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos).

**Objetivo**

Garantizar el cumplimiento e incorporación de los principios y deberes respecto a Protección de Datos Personales al Interior de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, estableciendo los componentes, procesos y requerimientos que deberán observarse en todo tratamiento de Datos Personales al interior de este sujeto obligado.

**Ámbito de aplicación**

El presente documento es de aplicación y observancia general y obligatoria para todas las personas servidoras públicas de la Comisión que conforme a sus atribuciones realicen tratamiento de datos personales.

# Glosario

**Activo:** La información, el conocimiento sobre los procesos, el personal, hardware, software y cualquier otro recurso involucrado en el tratamiento de los datos personales, que tenga valor para la organización.

**Amenaza:** Circunstancia o condición externa, con la capacidad de causar daño a los activos explotando una o más de sus vulnerabilidades.

**Análisis de brecha:** La concentración de elementos específicos que pueden existir entre lo deseable y lo actual. Para la realización del análisis de brecha, el responsable deberá considerar las medidas de seguridad existentes y efectivas, las medidas de seguridad faltantes y la existencia de nuevas medidas de seguridad que pudieran reemplazar a uno o más controles implementados actualmente.

**Análisis de riesgos:** La evaluación cuantitativa y cualitativa sobre la posibilidad de que un activo de información pueda sufrir una pérdida o daño. Contempla la identificación de activos, el estudio de causas y consecuencias de las amenazas y vulnerabilidades en los sistemas de tratamiento de datos personales, y permite establecer parámetros para ponderar los efectos de posibles vulneraciones de seguridad.

**Anonimización:** La aplicación de determinadas técnicas o procedimientos tendientes a impedir la identificación o reidentificación de una persona física sin que para ello sea necesario el empleo de esfuerzos desproporcionados.

**Archivo:** Al conjunto organizado de documentos producidos o recibidos por los sujetos obligados en el ejercicio de sus atribuciones y funciones, con independencia del soporte, espacio o lugar que se resguarden.

**Archivo de concentración:** Documentos que siguen siendo materia de consulta tanto para tomar decisiones como para dar respuesta a solicitudes de acceso a la información, pero que han pasado a esta segunda etapa de su ciclo de vida y, por ello, son consultados ocasionalmente.

**Archivo de trámite:** Al integrado por documentos de archivo de uso cotidiano y necesario para el ejercicio de las atribuciones y funciones de los sujetos obligados.

**Archivo histórico:** Al integrado por documentos de conservación permanente y de relevancia para la memoria nacional, regional o local de carácter público.

**Áreas o Unidades Administrativas:** Las áreas de adscripción que en su conjunto integran la estructura administrativa de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, establecidas y reconocidas en el artículo 4, del Estatuto Orgánico de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, así como aquellas áreas o unidades que por diversos cuerpos normativos y legislaciones aplicables tengan que existir; lo anterior, es aplicable aun aquellas áreas sin un acuerdo de creación o incorporación en la estructura, como la Unidad de Transparencia.

**Aviso de privacidad:** Documento a disposición del titular de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de estos.

**Baja documental:** Acción que consiste en la eliminación o destrucción de documentos cuyo plazo de conservación se extinguió y, por lo tanto, caducó su valor administrativo, legal, fiscal, contable e histórico.

**Bases de datos:** Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

**Bloqueo:** La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda.

**Comisión o CONDUSEF:** La Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros.

**CT o Comité de Transparencia:** El Comité de Transparencia de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros.

**Cómputo en la nube:** Almacenamiento y tratamiento de información -no solo personal- mediante una serie de tecnologías y modelos de servicio que se centran en el uso de internet y la prestación de aplicaciones informáticas, capacidad de tratamiento, espacio de memoria y almacenamiento.

**Confidencialidad:** Atributo de la información y al mismo tiempo un principio de seguridad que hace referencia a la obligación de que las personas que tienen acceso a ésta apliquen y respeten determinadas reglas y procedimientos a fin de que sea protegida de su divulgación no autorizada a terceros y se garantice que solo el personal autorizado pueda acceder a la misma.

**Consentimiento:** Manifestación de la voluntad libre, específica e informada del titular de los datos mediante la cual se efectúa el tratamiento de estos.

**CPEUM:** Constitución Política de los Estados Unidos Mexicanos.

**Datos personales:** Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

**Datos personales sensibles:** Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más, no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

**Datos personales biométricos:** Datos personales de carácter sensible referentes a las propiedades físicas, fisiológicas, de comportamiento o rasgos de la personalidad, mesurables y que conciernen a una persona física identificada o identificable.

**Derechos ARCOP:** Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.

- Derecho de **ACCESO:** la modalidad en la que prefiere que se reproduzcan los datos personales solicitados.
- Derecho de **RECTIFICACIÓN:** las modificaciones que solicita se realicen a los datos personales, así como aportar los documentos que sustenten la solicitud.
- Derecho de **CANCELACIÓN:** las causas que motivan la petición de que se eliminen los datos de los archivos, registros o bases de datos del responsable del tratamiento.

- Derecho de **OPOSICIÓN:** las causas legitimas o la situación que lo llevan a solicitar que finalice el tratamiento de sus datos personales, así como el daño o perjuicio que le causaría que dicho tratamiento continúe; o bien, las finalidades específicas respecto de las cuales desea ejercer este derecho.
- Derecho de **PORTABILIDAD:** 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.

**Disponibilidad:** Propiedad de un activo para ser accesible y utilizable cuando lo requieran personas, entidades o procesos autorizados.

**Documento de seguridad:** Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

**Encargado:** La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o juntamente con otras trate datos personales a nombre y por cuenta del responsable.

**Enlace de transparencia:** Las personas servidoras públicas designadas con tal carácter por las/los titulares de las Unidades Administrativas de la Comisión para atender las solicitudes que, en materia de transparencia, acceso a la información y protección de datos personales, asigne la Unidad de Transparencia y/o el Comité.

**Estatuto:** Estatuto Orgánico de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros.

**Fuentes de acceso público:** Aquellas bases de datos, sistemas o archivos que por disposición de ley puedan ser consultadas públicamente cuando no exista impedimento por una norma limitativa y sin más exigencia que, en su caso, el pago de una contraprestación, tarifa o contribución. No se considerará fuente de acceso público cuando la información contenida en la misma sea obtenida o tenga una procedencia ilícita, conforme a las disposiciones establecidas por la Ley y demás normativa aplicable.

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

**Incidente de seguridad:** Evento adverso o una violación a la política de seguridad de la información que compromete o puede comprometer la seguridad de la información implícita o explícitamente.

**Integridad:** La propiedad de salvaguardar la exactitud y completitud de los activos.

**Ley General o LGPDPPSO:** Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

**Lineamientos:** Lineamientos Generales de Protección de Datos Personales para el Sector Público.

**Medidas de seguridad:** Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.

**Medidas de seguridad administrativas:** Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales.

**Medidas de seguridad físicas:** Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.

**Medidas de seguridad técnicas:** Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento.

**Plazo de conservación:** Periodo de guarda de la documentación en los archivos de trámite y concentración, que consiste en la combinación de la vigencia documental y, en su caso, el término precautorio y periodo de reserva que se establezcan de conformidad con la normatividad aplicable.

**Protección de datos por defecto:** La obligación del responsable de aplicar medidas técnicas y organizativas apropiadas y orientadas a garantizar que, por defecto, esto es, por configuración ya previamente establecida del tratamiento, solo sean objeto de tratamiento los datos personales estrictamente necesarios para cada uno de los fines específicos del tratamiento, con independencia de la cantidad de datos personales recabados, el alcance del tratamiento, o el plazo de conservación, entre otros factores que se consideren relevantes por parte del responsable.

**Remisión:** Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano.

**Responsable:** Los sujetos obligados a que se refiere el artículo 1 de la Ley que deciden sobre el tratamiento de datos personales.

**Riesgo:** combinación de la probabilidad de que un incidente ocurra y de sus consecuencias desfavorables; de modo tal que, al determinar el riesgo en un escenario específico de la organización, se pueda evaluar el impacto y realizar un estimado de las medidas de seguridad necesarias para preservar la información personal.

**Supresión:** La baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable.

**Titular:** La persona física a quien corresponden los datos personales.

**Transferencia:** Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada con un tercero receptor.

**Tratamiento:** Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

**Unidad de Transparencia:** La Unidad de Transparencia de la CONDUSEF

## De los Principios

**Artículo 1.** El tratamiento de datos personales por parte de cada unidad administrativa se sujetará a las atribuciones o facultades que les son conferidas en la normatividad que rige el actuar de la CONDUSEF y, en estricto apego a lo dispuesto en la Ley General, los Lineamientos, la presente Política y demás disposiciones legales aplicables en materia de protección de datos personales.

**Artículo 2.** Las unidades administrativas de la CONDUSEF responsables del tratamiento de datos personales observarán los principios rectores, siguientes:

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

**Principio de Licitud**
**Artículo 3.** Previo a recabar datos personales, las unidades administrativas por conducto de los servidores públicos correspondientes deberán mostrar el aviso de privacidad.

**Artículo 4.** Al momento de recabar datos personales, se deberá hacer del conocimiento de la persona titular la finalidad con la cual se reciben de manera clara y precisa.

**Artículo 5.** Las unidades administrativas identificarán el marco normativo que en el ámbito de sus funciones se encuentra relacionado con el tratamiento de datos personales, el tipo de datos que tratan y las finalidades para ello, incluyéndolo en el Aviso de Privacidad y los Inventarios de datos y sistemas de Tratamientos del área.

**Artículo 6.** Bajo el entendido de que todos los datos personales tienen que ser tratados de manera lícita, esto es, debe sujetarse a las facultades o atribuciones que la normatividad aplicable le otorga, las unidades administrativas deberán observar:

I. Revisar que los datos se traten conforme a la LGPDPPSO, Lineamientos Generales y demás normativa aplicable.
II. Conocer la normativa que en lo particular regule sus atribuciones, funciones y responsabilidades con relación al tratamiento de los datos personales que realice.
III. Incluir previsiones sobre la obligación de cumplir con este principio en las cláusulas, contratos u otros instrumentos jurídicos que se firmen con terceros.

**Principio de Finalidad**
**Artículo 7.** Todo tratamiento de datos personales efectuado por las áreas deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas.

Para dicho efecto, se entenderá que las finalidades son:

I. 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;

II. Explícitas: cuando las finalidades se expresan y dan a conocer de manera clara en el aviso de privacidad;
III. 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
IV. 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.

**Artículo 8.** Como consecuencia del principio de finalidad, las unidades administrativas que traten datos personales deberán:

I. Establecer detalladamente en el aviso de privacidad todas las finalidades para las cuales se tratarán los datos personales, las cuales serán acordes a las atribuciones o facultades que tienen encomendadas;
II. Tratar los datos personales únicamente para la finalidad o finalidades que hayan sido informadas a la persona titular en el aviso de privacidad y, en su caso, consentidas por ésta;
III. Obtener el consentimiento de los titulares para el tratamiento de sus datos personales, salvo las excepciones establecidas en el artículo 22 de la Ley General;
IV. Identificar y distinguir en el aviso de privacidad entre las finalidades primarias y secundarias;
V. Ofrecer a la persona 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;
VI. Cuando el aviso de privacidad se dé a conocer a través de un medio indirecto, informar a la persona titular que tiene cinco días hábiles para manifestar su negativa para el tratamiento de su información para finalidades secundarias; y
VII. No condicionar el tratamiento para finalidades primarias, a que se puedan llevar a cabo las finalidades secundarias.

**Artículo 9.** Para acreditar el cumplimiento del principio de finalidad, las áreas deberán:

I. Incluir en el inventario, las finalidades de cada tratamiento que se realice en su unidad administrativa y verificar que estas sean específicas o determinadas y que sean acordes a las atribuciones o facultades de la Comisión y de su área.
II. Vigilar que los servidores públicos Únicamente traten datos personales en términos de las finalidades informadas en el aviso de privacidad correspondiente.
III. Verificar que en los avisos de privacidad se informen todas las finalidades para las cuales se tratan los datos personales, y que éstas sean descritas de manera clara.
IV. Informar a los titulares sobre el tratamiento de los datos para finalidades distintas.
V. Recabar el consentimiento de los titulares, cuando este proceda.

**Principio de Lealtad**
**Artículo 10.** Las unidades administrativas de la CONDUSEF se abstendrán de obtener y tratar datos personales a través de medios engañosos o fraudulentos, privilegiando la protección de los intereses del titular y la protección de datos personales por defecto.

**Artículo 11.** Derivado del principio de lealtad los servidores públicos responsables del tratamiento de datos personales deberán:

I. Obtener y tratar los datos personales sin que medie dolo, mala fe o negligencia;
II. Privilegiar los intereses del titular y, evitar cualquier tipo discriminación, trato injusto o arbitrario en contra de éstos, con motivo del tratamiento de sus datos;

III. Revisar los procedimientos y formatos utilizados para recabar datos personales, para verificar que en éstos no se utilicen prácticas que lleven a la obtención de los datos de manera dolosa, de mala fe o con negligencia;
IV. Dar vista al Órgano Interno de Control en caso del uso de prácticas dolosas, de mala fe o negligentes para la obtención de los datos personales;
V. Respetar en todo momento la expectativa razonable de privacidad de la persona titular de los datos personales;
VI. Tratar los datos conforme lo acordado e informado a la persona titular de los datos personales;
VII. Verificar los tratamientos, a fin de confirmar que los mismos no den lugar a discriminación o trato injusto o arbitrario en contra del titular;
VIII. Elaborar avisos de privacidad con todos los elementos informativos que establece la LGPDPPSO, y con información que corresponda a la realidad del tratamiento que se efectúa; y
IX. 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.

**Artículo 12.** Para acreditar el cumplimiento del principio de lealtad, las unidades administrativas deberán:

I. Contar con avisos de privacidad publicados y actualizados que cumplan con lo establecido en la Ley General y los Lineamientos.
II. Implementar instrumentos que permitan verificar que los tratamientos realizados no den lugar a discriminación, trato injusto o arbitrario en contra del titular.
III. Constatar que el tratamiento de datos personales sólo se lleve a cabo para los fines informados en el aviso de privacidad.

**Principio de Consentimiento.**
**Artículo 13**. Previo al tratamiento de los datos personales, las áreas obtendrán el consentimiento del titular de manera libre, específica e informada, en términos de lo dispuesto en la Ley General, salvo que se actualice alguna de las causales de excepción siguientes:

I. 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.
II. Cuando las transferencias que se realicen entre la CONDUSEF 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.
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 la CONDUSEF.
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 necesarios para efectuar un tratamiento para la prevención, diagnóstico o 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.
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 no exime al área y a los servidores públicos responsables del tratamiento de datos personales del cumplimiento de las demás obligaciones establecidas en la Ley General, los Lineamientos, el presente documento y demás normativa en la materia.

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, por escrito cuando se refiera a datos sensibles.

**Artículo 14.** En términos de los alcances del principio de consentimiento, las unidades administrativas deberán:

I. Identificar las finalidades para las cuales se requiere el consentimiento de los titulares;
II. Obtener el consentimiento del titular, previo al tratamiento de los datos, salvo que se actualice alguno de los supuestos de excepción descritos en el artículo anterior.
III. Recabar el consentimiento expreso y, en su caso, por escrito, a través de formatos que deben ser redactados de forma tal que éste sea libre, específico e informado, y que sean concisas e inteligibles, estén en un lenguaje claro y sencillo acorde con el perfil del titular, en los cuales se distingan los datos y finalidades del tratamiento que requieren de la manifestación de su voluntad.
IV. 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.
V. Implementar medios sencillos y gratuitos para la obtención del consentimiento, independientemente de la modalidad en que éste se requiera.
VI. Cuando los datos personales no los proporcione personal o directamente el titular o su representante, 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, entonces podrá suponer que cuenta con el consentimiento tácito.

**Artículo 15.** Para acreditar el cumplimiento del principio de consentimiento, las unidades administrativas deberán:

I. Identificar en el aviso de privacidad, aquellos datos y finalidades que requieren del consentimiento del titular, para su tratamiento.
II. Mantener bajo su resguardo una copia del documento en el cual se haya manifestado el consentimiento del titular para el tratamiento de sus datos, cuando éste proceda.
III. Documentar la puesta a disposición del aviso de privacidad al titular, en aquellos casos en los cuales sea válido el consentimiento tácito.

**Artículo 16.** Independientemente de que se requiera o no el consentimiento del titular para el tratamiento de sus datos personales, las áreas de la CONDUSEF informarán a los titulares sobre la existencia y las características principales del tratamiento al que serán sometidos sus datos personales.

**Principio de Información**
**Artículo 17**. Las áreas que realizan tratamientos de datos personales se encuentran obligadas a informar a las personas titulares de los datos personales, a través de los avisos de privacidad integral y simplificado, las Características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.

**Artículo 18.** Para dar atención al principio de información, las unidades administrativas que traten datos personales deberán:

I. Poner a disposición de los titulares el aviso de privacidad en los términos dispuestos en la LGPDPPSO, y demás normativa aplicable.

II. Poner gratuitamente a disposición de los titulares el aviso de privacidad en los términos que fije la Ley General y los Lineamientos Generales, aunque no se requiera el consentimiento de los titulares para el tratamiento de los datos personales.
III. Elaborar los avisos de privacidad con todos los elementos informativos que resulten aplicables, de manera clara, comprensible, así como con una estructura y diseño que facilite su entendimiento, considerando su accesibilidad para personas con algún tipo de discapacidad.
IV. Difundir el aviso de privacidad por medios electrónicos y físicos.
V. Ubicar el aviso de privacidad en un lugar visible y que facilite su consulta, con independencia del medio de difusión o reproducción que se utilice.
VI. Poner a disposición de la persona titular el aviso de privacidad previo a iniciar el uso de los datos personales para la finalidad para la que se obtuvieron, cuando éstos no se hayan obtenido de manera directa de la titular, el tratamiento no requiera del contacto con ésta y se cuente con datos para contactarle.
VII. Comunicar el aviso de privacidad a quienes se transfieran datos personales.
VIII. Prever la implementación de medidas compensatorias, en términos de lo dispuesto en la Ley General y demás disposiciones aplicables, para dar a conocer los avisos de privacidad a través de medios masivos de difusión cuando resulte imposible hacerlo de manera directa al titular o, ello exija esfuerzos desproporcionados.
IX. Poner a disposición del titular el aviso de privacidad previo a iniciar el uso de los datos personales para las nuevas finalidades (aprovechamiento), cuando requiera tratar los datos personales para finalidades distintas y no compatibles con aquéllas para las cuales los recabó inicialmente.

**Artículo 19.** Para acreditar el cumplimiento del principio de información, las unidades administrativas cumplirán con las siguientes acciones:

I. Contar con los avisos de privacidad integral y simplificado por cada proceso de tratamiento de datos personales que se lleve a cabo, publicados en el apartado de protección de datos personales de esta Comisión.
II. Incluir en el inventario los lugares y medios en los que se difunden y colocan los avisos de privacidad.
III. Documentar la comunicación realizada del aviso de privacidad a terceros a los que se transfieran los datos personales.
IV. Demostrar el cumplimiento del principio de información, en caso de que así se requiera.

**Principio de Proporcionalidad.**
**Artículo 20.** Las áreas de la CONDUSEF recabarán aquellos datos personales que 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.

**Artículo 21.** Para el cumplimiento del principio de proporcionalidad los servidores públicos responsables del tratamiento de datos personales deberán:

I. Recabar y tratar sólo aquellos datos personales necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron.
II. Realizar esfuerzos razonables para actualizar la normativa y formatos internos, con el fin de 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. 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.

V. Crear bases de datos con datos personales sensibles sólo cuando:

a) Obedezca a un mandato legal;
b) Se justifique para la seguridad nacional, el orden, la seguridad y la salud públicos, así como
b) derechos de terceros, o
c) Lo requiera para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persiga.

**Artículo 22.** A fin de acreditar el cumplimiento del principio de proporcionalidad, las unidades administrativas realizarán, al menos:

I. 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.
II. Promover que en su área se requiera el mínimo posible de datos personales para lograr las finalidades para las cuales se tratan.
III. Promover prácticas que minimicen la obtención de datos personales y el periodo de su tratamiento, así como señalarlas en el documento de seguridad.

**Principio de Calidad**
**Artículo 23.** Para el cumplimiento del principio de calidad, las unidades administrativas deberán tener en cuenta que conforme a la finalidad o finalidades para las que se vayan a tratar los datos personales, éstos deben ser:

I. Exactos y correctos: Cuando los datos personales no presentan errores que pudieran afectar su veracidad.
II. Completos: Cuando su integridad permite el cumplimiento de las finalidades que motivaron su tratamiento y las atribuciones del responsable.
III. Pertinentes: Cuando corresponden efectivamente a su titular.
IV. Actualizados: Cuando los datos personales responden fielmente a la situación actual del titular.

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

Cuando los datos personales se hayan obtenido indirectamente del titular, las áreas adoptarán las medidas pertinentes para garantizar que éstos respondan al principio de calidad, de acuerdo con la categoría de datos personales, así como las condiciones y medios del tratamiento.

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 de éstos, en los términos previstos en el inventario de datos personales.

**Artículo 24.** Para el cumplimiento del principio de calidad, las unidades administrativas que traten datos personales deberán:

I. Adoptar las medidas que considere convenientes para procurar que los datos personales cumplan con las características de ser exactos, completos, pertinentes, actualizados y correctos, a fin de que no se altere la veracidad de la información, ni que ello tenga como consecuencia que la persona titular se vea afectada por dicha situación.
II. Establecer plazos de conservación de la información, conforme a las disposiciones legales aplicables en materia archivística.

III. Bloquear los datos personales antes de suprimirlos, y durante el periodo de bloqueo sólo tratarlos para su almacenamiento y acceso en caso de que se requiera determinar posibles responsabilidades en relación con el tratamiento de los datos personales.
IV. Elaborar procedimientos para la conservación, bloqueo y supresión de los datos personales.

**Artículo 25.** Para acreditar el cumplimiento del principio de calidad, las unidades administrativas deberán atender lo siguiente:

I. Contar con 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 y actualizarlas.
II. Documentar las actualizaciones y supresiones realizadas.
III. Contar con los procedimientos para la conservación, bloqueo y supresión de los datos personales.

**Principio de Responsabilidad**
**Artículo 26**. Conforme al principio de responsabilidad, la CONDUSEF velará por el cumplimiento del resto de los principios; promoverá la adopción de medidas necesarias para su aplicación y, demostrará ante titulares y el organismo garante, que se cumplen con las obligaciones en torno a la protección de los datos personales.

**Artículo 27**. Para dar cumplimiento al principio de responsabilidad, las unidades administrativas efectuarán lo siguiente:

I. Prever recursos para la instrumentación de la presente Política y del programa de protección de datos, en su caso.
II. Incentivar la capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales.
III. Revisar periódicamente el programa de protección de datos personales y el documento de seguridad para determinar las modificaciones que se requieran.
IV. Establecer procedimientos para recibir y responder dudas y quejas de los titulares.
V. Analizar los riesgos que implica todo tratamiento de datos personales.

**Artículo 28.** Para acreditar el cumplimiento al principio de responsabilidad, las unidades administrativas deberán:

I. Contar con las constancias de capacitación de su personal en temas relacionados con la materia de protección de datos personales.
II. Atender a los procedimientos de las dudas y quejas de los titulares, y llevar un registro.
III. Documentar la comunicación hacia su personal de la presente Política y del programa de protección de datos que al efecto sea aprobado.
IV. Guardar evidencia del cumplimiento a las acciones mencionadas.

## De los deberes

**Artículo 29.** Además de los principios señalados en el Capítulo anterior, las áreas cumplirán con las acciones necesarias para el cumplimiento de los deberes:

I. Deber de confidencialidad
II. Deber de seguridad

**Deber de Confidencialidad**
**Artículo 30.** Las áreas establecerán controles o mecanismos de observancia obligatoria para los servidores públicos que intervengan en cualquier fase del tratamiento, con la finalidad de que éstos guarden

confidencialidad de los datos personales, obligación que subsistirá aún después de finalizar su relación laboral con la CONDUSEF y sin menoscabo de lo establecido en las disposiciones de acceso a la información pública.

**Artículo 31.** Para el debido cumplimiento del deber de confidencialidad, la Unidad de Transparencia deberá:

I. Prever controles mediante los cuales se garantice la confidencialidad de los datos personales que son tratados.
II. Implementar campañas de sensibilización para los servidores públicos, sobre la importancia de la confidencialidad de los datos personales.
III. Proponer al Comité de Transparencia la implementación de mejores prácticas al interior de la CONDUSEF para garantizar la secrecía de los datos personales.
IV. Socializar al interior de la CONDUSEF la carta de confidencialidad, y solicitar a las áreas un registro de los servidores públicos que en facultad de sus labores intervengan en el tratamiento de datos personales y efectivamente hayan firmado la carta.
V. Solicitar la capacitación del personal para que conozca sus obligaciones con relación al tratamiento de datos personales al Instituto o ante el área de Capacitación de la CONDUSEF.
VI. Proponer al Comité procedimientos para evitar fuga de información o el acceso indebido a los datos personales.
VII. Proponer al Comité la realización de verificaciones o supervisiones periódicas al trabajo realizado por los encargados, a fin de verificar que se cumplan con sus obligaciones en torno a la protección de los datos personales.

**Artículo 32.** Asimismo, las áreas deberán:

I. 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;
II. Guardar confidencialidad en cualquier fase del tratamiento de los datos personales, incluso después de finalizar la relación con la persona titular;
III. Verificar que los encargados también guarden confidencialidad de los datos personales que tratan a nombre y por cuenta del responsable, aun después de concluida la relación con éste;
IV. Cumplimentar los procedimientos para evitar fuga de información o el acceso indebido a los datos personales que para el efecto apruebe el Comité de Transparencia.

**Artículo 33.** Para acreditar el cumplimiento del deber de confidencialidad, las unidades administrativas realizarán, al menos, lo siguiente:

I. Implementar medidas de seguridad para garantizar la secrecía de los datos personales.
II. Realizar el registro de los servidores públicos que en facultad de sus labores intervengan en el tratamiento de datos personales y efectivamente hayan firmado la carta.
III. Contar con los contratos en los cuales se establezcan las cláusulas de confidencialidad de datos, respecto de transferencias o remisiones.
IV. Tener la evidencia documental de los cursos, talleres, seminarios o similar en los que haya participado el personal de la unidad administrativa y se encuentre relacionado con la materia de protección de datos personales.
V. Documentar la implementación de mejores prácticas que garanticen la confidencialidad de los datos tratados.

**Deber de Seguridad**
**Artículo 34.** Las áreas adoptarán e instrumentarán las medidas de seguridad físicas, técnicas y administrativas a través de las cuales se garantice la protección de los datos personales tratados, a fin de evitar cualquier afectación a estos y su titular.

**Artículo 35.** Para el debido cumplimiento del deber de seguridad, las unidades administrativas deberán:

I. Actualizar el Inventario de Datos personales que integra el Documento de Seguridad de esta Comisión sin omitir el tipo de datos personales recabados, el tratamiento que se les dará y el ciclo de vida de estos.
II. Establecer los servidores públicos que podrán intervenir en el tratamiento de los datos personales y definir las funciones y obligaciones que estos tendrán.
III. Realizar un análisis de riesgo de los datos personales tratados, así como de los sistemas físicos y/o electrónicos en el cual se desarrolle dicho tratamiento.
IV. Desarrollar acciones de prevención y mitigación de amenazas o vulneraciones de datos personales.
V. Monitorear y revisar de las medidas de seguridad adoptadas para garantizar la protección de datos.
VI. Incentivar la capacitación de los servidores públicos involucrados en el tratamiento de datos personales, conforme al nivel de responsabilidad que éstos tengan asignado.

**Artículo 36.** Para acreditar el cumplimiento del deber de seguridad, las unidades administrativas realizarán, al menos, lo siguiente:

I. Contar con un inventario de datos y de los sistemas de tratamiento actualizado.
II. Comunicar al personal las políticas implementadas para la protección de datos y guardar evidencia de ello.
III. 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.
IV. 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.
V. Tener la evidencia documental de los cursos, talleres, seminarios o similar en los que haya participado el personal del área y se encuentre relacionado con la materia de protección de datos personales.

## Del Programa de Protección de Datos Personales

**Artículo 37.** La CONDUSEF contará con un programa de protección de datos personales que se denominará Cronograma de implementación de la LGPDPPSO, aprobado por el Comité de Transparencia, cuyo objetivo es determinar las pautas generales bajo las cuales se llevarán a cabo las tareas institucionales orientadas a mantener la observancia en el cumplimiento de los principios y deberes, así como a garantizar el derecho a la protección de datos personales al interior de este sujeto obligado.

**Artículo 38.** El cronograma tendrá una vigencia de un año, contemplando que debe realizarse en continuación al Cronograma del ejercicio fiscal anterior.

**Artículo 39.** La Unidad de Transparencia elaborará la propuesta de ajustes o actualizaciones al programa de protección de datos personales de la CONDUSEF, las cuales serán presentadas al Comité de Transparencia para su revisión y, en su caso, aprobación.

**Artículo 40.** El Programa de Protección de Datos Personales de la CONDUSEF deberá contener al menos:

I. La vigencia del programa.
II. Un diagnóstico sobre los problemas, necesidades o áreas de oportunidad detectadas para el debido cumplimiento de los principios y deberes en materia de protección de datos personales dentro de la CONDUSEF.

III. Las actividades propuestas, su viabilidad, así como los objetivos que se persiguen, los cuales estarán vinculados a la atención de los problemas, necesidades o áreas de oportunidad previamente detectadas.

**Artículo 41.** Corresponde al Comité de Transparencia dar seguimiento al cumplimiento de las acciones propuestas en el programa de protección de datos personales y sus resultados.

## De los Enlaces

**Artículo 42.** Todas las unidades administrativas designarán a un servidor público cuyo encargo será fungir al interior del área, así como ante la Unidad de Transparencia y el Comité de Transparencia, como enlace responsable de las actividades en materia de protección de datos personales, con el fin de garantizar y evidenciar la operación y cumplimiento de esta Política ante el titular y el INAI. En caso de no hacer los nombramientos respectivos, se guardará comunicación, para el desahogo de esta materia, con los enlaces de transparencia.

**Artículo 43.** Serán funciones de los enlaces en materia de protección de datos personales al interior de esta Comisión:

I. Gestionar al interior de su unidad administrativa, la debida atención de solicitudes relativas al ejercicio de los Derechos ARCOP que sean presentadas ante la Unidad de Transparencia.
II. Promover la capacitación de los servidores públicos al interior de su unidad administrativa y que se encuentren involucrados directamente en el tratamiento de datos personales.
III. Participar en la integración y actualización de los documentos integradores del Documento de Seguridad.
IV. Validar y, en su caso, actualizar semestralmente el inventario de datos personales que, en el ámbito de su competencia, correspondan a su unidad administrativa.
V. Socializar todas aquellas invitaciones, o comunicaciones relevantes que la Unidad de Transparencia o el Comité de Transparencia les remita.
VI. Las demás que determinen las disposiciones normativas, el INAI o, aquellas que deriven de las resoluciones emitidas por el Comité de Transparencia.

## Del Documento de Seguridad

**Artículo 44.** La CONDUSEF cuenta con un Documento de Seguridad como parte de los mecanismos implementados para asegurar el cumplimiento al deber de seguridad, cuyo objeto es establecer, de manera general, las medidas de seguridad técnicas, físicas y administrativas adoptadas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales tratados.

**Artículo 45.** 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.
VII. El programa general de capacitación.

**Artículo 46.** En las actualizaciones que se realicen al Documento de Seguridad deberán participar todas las unidades administrativas, a través de los enlaces que para los efectos sean nombrados, quienes en todo

momento observarán los principios y deberes a que se refiere la Ley General, los Lineamientos y demás disposiciones legales aplicables.

Para la formulación de propuestas de actualización del Documento de Seguridad, la Unidad de Transparencia elaborará formatos, cuestionarios o cualquier otro instrumento de apoyo, que resulte útil para el cumplimiento de las obligaciones mencionadas en la legislación aplicable en la materia.

Acorde 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 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.

**Artículo 47.** Cuando alguna de las áreas se encuentre en cualquiera de los supuestos referidos, el enlace responsable solicitará por escrito al Comité de Transparencia las actualizaciones correspondientes, quien resolverá lo conducente.

Los enlaces responsables podrán solicitar orientación técnica a la Unidad de Transparencia, para la integración o cualquier acto relacionado con los alcances del Documento de Seguridad.

**Artículo 48.** Corresponde al titular de cada unidad administrativa y al personal de mando superior la supervisión de las políticas internas para la gestión y tratamiento de datos personales de su área.

**Artículo 49.** En términos de lo previsto en la Ley General, se consideran vulneraciones a la seguridad de los datos, 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.
IV. El daño, la alteración o modificación no autorizada.

**Artículo 50.** Cuando las vulneraciones afecten de forma significativa los derechos patrimoniales o morales de los titulares, las unidades administrativas involucradas, deberán generar un informe detallado que contenga al menos lo siguiente:

I. La naturaleza del incidente.
II. Los datos personales comprometidos.
III. Las recomendaciones al titular acerca de las medidas que éste puede adoptar para proteger sus intereses.
IV. Las acciones correctivas implementadas para mitigar la vulneración.
V. Los datos de contacto del enlace responsable o personal al cual puede acudir el titular para obtener más información al respecto.

Dicho informe se deberá informar a los titulares afectados, a fin de que puedan tomar las medidas correspondientes para la defensa de sus derechos y a la Unidad de Transparencia sin dilación alguna[1], para que ésta lo haga del conocimiento del INAI y del Comité de Transparencia.

Adicionalmente, las unidades administrativas deberán prever en el informe a notificarse al INAI por parte de la Unidad de Transparencia, lo siguiente:

a. La hora y fecha de la identificación de la vulneración.
b. La hora y fecha del inicio de la investigación sobre la vulneración.
c. La naturaleza del incidente o vulneración ocurrida.
d. La descripción detallada de las circunstancias en torno a la vulneración ocurrida.
e. Las categorías y número aproximado de titulares afectados.
f. Los sistemas de tratamiento y datos personales comprometidos.
g. La descripción de las posibles consecuencias de la vulneración de seguridad ocurrida.
h. Cualquier otra información y documentación que considere conveniente hacer del conocimiento del Instituto.

**Artículo 51.** Conforme a lo previsto en los Lineamientos, se entenderá que afectan los derechos patrimoniales del titular, cuando la vulneración esté relacionada con sus bienes, información fiscal, historial crediticio, ingresos o egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados u otros similares.

Para el caso de los derechos morales, se entenderán aquellos relacionados, de manera enunciativa con sus sentimientos, afectos, creencias, decoro, honor, reputación, vid privada, aspecto físico o menoscabe ilegalmente la libertad, integridad física o psíquica del titular de los datos.

**Artículo 52.** En aquellos casos en los cuales no sea posible notificar directamente a los titulares de los datos el informe a que hace referencia la presente Política o ello implique esfuerzos desproporcionados, las áreas instrumentarán medidas compensatorias de comunicación para tal efecto, como son: la publicación en periódico oficial, página de Internet, carteles o cápsulas informativas u otro similar.

**Artículo 53.** El Comité de Transparencia podrá determinar la implementación de acciones adicionales a las realizadas por las unidades administrativas para evitar futuras vulneraciones y reforzar las medidas de seguridad aplicables.

Para tal efecto, el Comité de Transparencia podrá auxiliarse de la asesoría, orientación o apoyo de otras unidades administrativas de la CONDUSEF, proponer la suscripción de convenios de colaboración o solicitar la contratación de especialistas en la materia, siempre y cuando exista la suficiencia presupuestal para ello.

## De los Avisos de Privacidad

**Artículo 54.** Como parte de las acciones para cumplir con el principio de información y, con independencia de que no se requiera del consentimiento del titular para el tratamiento de sus datos personales, todas las áreas de la Comisión contarán con un aviso de privacidad integral y su correlativo aviso de privacidad simplificado, por cada proceso en los que traten datos personales.

Excepcionalmente, cuando dos o más procesos de tratamiento de datos personales, atiendan a 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.

[1] El plazo máximo para notificar las vulneraciones es de 72 horas, a partir de que el responsable confirme las vulneraciones ocurridas. Artículo 66 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

**Artículo 55.** Los formatos para la elaboración de los avisos de privacidad integral y simplificado serán acordes con los elementos que establece la Ley General, los Lineamientos y demás normatividad que resulte aplicable.

**Artículo 56.** En la integración y elaboración de los avisos de privacidad, las unidades administrativas preverán un diseño que facilite su entendimiento por parte de los titulares de los datos.

**Artículo 57.** Las unidades administrativas se asegurarán de que la información asentada en los avisos de privacidad se encuentre redactada en un lenguaje sencillo, claro y comprensible, considerando en todo momento el perfil del 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 titulares a elegir una opción en específico.
III. Marcar previamente casillas, en caso de que éstas se incluyan, para que los titulares otorguen su consentimiento, o bien, incluir declaraciones orientadas a afirmar que el titular 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 los titulares.

**Artículo 58.** Para la elaboración o actualización de los avisos de privacidad, los enlaces responsables podrán en todo momento, solicitar orientación técnica a la Unidad de Transparencia.

**Artículo 59.** En sustitución de los avisos de privacidad ya existentes, los servidores públicos responsables, considerarán la elaboración de un nuevo aviso de privacidad, en sus dos modalidades cuando:

I. Por disposición del Estatuto, el proceso de tratamiento de datos personales se traslade a una nueva área o ésta cambie su denominación.
II. Se requieran recabar datos sensibles a aquellos informados en el aviso de privacidad original, los cuales no se obtengan de manera directa del titular y se requiera de su consentimiento para el tratamiento de estos.
III. Cambien las finalidades señaladas en el aviso de privacidad original, o
IV. Se modifiquen las condiciones de las transferencias de datos personales o se pretendan realizar otras no previstas inicialmente y, el consentimiento del titular sea necesario.

**Artículo 60.** De manera anual la Unidad de Transparencia requerirá a las áreas para evaluar si es necesaria una
actualización de los datos personales con lo que se cuenta.

## Del Programa de Capacitación y Actualización

**Artículo 61.** La CONDUSEF 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 a los roles y responsabilidades de los servidores públicos que tratan la información personal.

**Artículo 62.** 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 le sea presentada por la Unidad de Transparencia, en la cual se consideren las necesidades de capacitación de las unidades administrativas y la oferta educativa del INAI.

El Comité de Transparencia y las áreas podrán proponer al área de capacitación la incorporación y coordinación de programas o actividades de capacitación en la materia, para su consideración en el Programa Anual de Capacitación de la CONDUSEF.

**Artículo 63.** En caso de que los cursos y actividades de capacitación corresponda a contenidos ofertados por el INAI, la Unidad de Transparencia será la encargada de remitir la invitación a los enlaces, lo cual se comunicará al área de capacitación para los efectos conducentes.

## Del Ejercicio de los Derechos ARCOP

**Artículo 64.** Para efectos de este procedimiento, se considera que los derechos ARCOP comprenden:

I. Acceso: Derecho del titular para acceder a sus datos personales en posesión de la CONDUSEF, así como conocer la información relacionada con las condiciones y generalidades de su tratamiento.
II. Rectificación: Derecho del titular para solicitar a la CONDUSEF la corrección de sus datos personales, cuando estos resulten inexactos, incompletos o no se encuentren actualizados.
III. Cancelación: Derecho del titular para solicitar a la CONDUSEF que sus datos personales sean bloqueados y, posteriormente, suprimidos de los archivos, registros, expedientes y sistemas institucionales de la
IV. CONDUSEF, a fin de que los mismos no se encuentren más en su posesión y, por lo tanto, dejen de ser tratados.
V. Oposición: Derecho del titular para solicitar a la CONDUSEF que se abstenga de utilizar información personal para ciertos fines o de requerir que se concluya su uso, a fin de evitar un daño o afectación a su persona.
V. Portabilidad[2]: Prerrogativa de los titulares que 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.

**Artículo 65.** La presentación de solicitudes de derechos ARCOP podrá realizarse a través de los medios de recepción siguientes:

I. Unidad de Transparencia ubicada en Avenida de los Insurgentes Sur 762, Planta Baja, Colonia Del Valle, Alcaldía Benito Juárez, en la Ciudad de México, C.P. 03100.
II. Correo electrónico: transparencia@condusef.gob.mx; y
III. Plataforma Nacional de Transparencia: http://www.plataformadetransparencia.org.mx/

**Artículo 66.** La Unidad de Transparencia será la responsable de turnar las solicitudes de ejercicio de derechos ARCOP que sean presentadas a la CONDUSEF a aquellas áreas que conforme a sus atribuciones, competencias o funciones puedan o deban poseer los datos personales se pronuncien, para dar atención a estas en los plazos y términos establecidos en la Ley General, los Lineamientos, los Lineamientos Internos y demás disposiciones aplicables en la materia, asimismo, la Unidad de Transparencia deberá emitir el documento que contenga los procedimientos internos para la atención de los Derechos ARCOP.

**Artículo 67.** Las unidades administrativas llevarán a cabo las acciones pertinentes para garantizar el efectivo ejercicio de los Derechos ARCOP de los titulares, acorde con los principios, obligaciones y deberes en materia de protección de datos personales.

[2] El derecho de portabilidad se encuentra contemplado en el presente documento en cumplimiento a la normatividad vigente en materia de protección de datos personales, sin embargo, es necesario mencionar que actualmente está CONDUSEF no cuenta con tratamientos que prevean la acción del derecho de portabilidad de datos personales

**Artículo 68.** Las áreas cooperarán con la Unidad de Transparencia para la atención de las solicitudes y, en su caso, para la formulación de alegatos derivados de los recursos de revisión interpuestos en términos de la Ley General, con motivo de las respuestas otorgadas,

**Artículo 69.** La resolución que emita el Instituto es vinculante para la CONDUSEF y, una vez recibida, la Unidad de Transparencia llevará a cabo las gestiones que resulten necesarias ante las unidades administrativas competentes para dar cumplimiento a lo instruido.

## De las Remisiones y Transferencias de los Datos Personales en posesión de la CONDUSEF

**Artículo 70.** La remisión es toda aquella comunicación de datos personales realizada exclusivamente entre responsables (CONDUSEF) y encargado, dentro o fuera del territorio mexicano.

**Artículo 71.** La CONDUSEF podrá encargar el tratamiento de datos personales a personas físicas o morales ajenas a la institución, únicamente cuando sea consecuencia de la existencia de una relación formalizada mediante un instrumento jurídico suscrito por los servidores públicos facultados para ello.

**Artículo 72.** El encargado tratará los datos personales a nombre y por cuenta de la CONDUSEF dentro del ámbito de actuación de la prestación del servicio debidamente formalizado y sin ostentar poder alguno de decisión sobre el alcance y contenido del tratamiento, limitando en ese sentido, sus actuaciones a los términos fijados por la Comisión,

**Artículo 73.** Cualquier acuerdo alcanzado y debidamente formalizado entre la CONDUSEF y el encargado se efectuará con base en lo previsto por la Ley General, los Lineamientos, la presente Política y el aviso de privacidad puesto a disposición de los titulares,

**Artículo 74.** Acorde con lo dispuesto en la Ley General y los Lineamientos, el instrumento jurídico por el cual se formalice la relación jurídica entre esta Comisión y el encargado deberá incluir al menos las siguientes obligaciones para este:

I. Realizar el tratamiento de los datos personales conforme a las instrucciones de la CONDUSEF.
II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por la CONDUSEF.
III. Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables.
IV. Informar a la CONDUSEF cuando ocurra una vulneración a los datos personales que trata por sus instrucciones,
V. Guardar confidencialidad respecto de los datos personales tratados.
VI. Suprimir o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con la CONDUSEF, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales.
VII. 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.
VIII. Permitir al INAI o a la Comisión, realizar verificaciones en el lugar o establecimiento donde se lleva a cabo el tratamiento de los datos personales.
IX. Colaborar con el INAI en las investigaciones previas y verificaciones que lleve a cabo en términos de lo dispuesto en la Ley General y los Lineamientos, proporcionando la información y documentación que se estime necesaria para tal efecto.
X. Generar, actualizar y conservar la documentación necesaria que le permita acreditar el cumplimiento de las obligaciones señaladas en este artículo.

**Artículo 75.** La subcontratación de servicios que impliquen el tratamiento de los datos personales previamente remitidos por la CONDUSEF sólo podrá llevarse a cabo cuando en el instrumento jurídico suscrito por la CONDUSEF y el encargado se contemple dicha situación, debiendo el encargado formalizar, a su vez, la relación jurídica con el subcontratado a través de cualquier instrumento jurídico que permita acreditar su existencia, alcance y contenido, en términos de las disposiciones legales aplicables.

En el instrumento jurídico de subcontratación, además de prever las cláusulas establecidas en el artículo anterior, se establecerá que la persona física o moral subcontratada asumirá las mismas obligaciones establecidas para el encargado.

**Artículo 76.** La CONDUSEF podrá contratar o adherirse a servicios, aplicaciones e infraestructura en el cómputo en la nube y otras materias que impliquen el tratamiento de datos personales, siempre y cuando el proveedor externo garantice las condiciones y cuente con los mecanismos establecidos en la LGPDPPSO.

Para dichos efectos, el área contratante deberá solicitar un dictamen técnico al área que, de conformidad con las atribuciones establecidas en la normativa interna, cuente con la atribución de establecer normas y emitir las políticas en materia de tecnología de la información, comunicación y seguridad informática en la CONDUSEF.

## De las Transferencias de Datos Personales

**Artículo 77.** La CONDUSEF podrá llevar a cabo transferencias nacionales o internacionales a terceros, de los datos personales en su posesión en los términos y bajo las condiciones que determina la Ley General.

Las comunicaciones de los datos personales que lleve a cabo la CONDUSEF a los encargados, no serán consideradas como transferencias.

**Artículo 78.** Toda transferencia de datos personales que lleve a cabo la CONDUSEF se encuentra sujeta al consentimiento de su titular, para tal efecto, las unidades administrativas de la CONDUSEF por medio del aviso de privacidad correspondiente informarán al titular de los datos personales, las finalidades de la transferencia, así como su destinatario.

En caso de ser una transferencia que requiera de consentimiento, se habilitarán los mecanismos para que el titular manifieste la voluntad correspondiente.

La Comisión no estará obligada a requerir el consentimiento del titular para llevar a cabo la transferencia de sus datos, en los casos previstos por la Ley General. La actualización de alguna de las excepciones previstas en las disposiciones previamente citadas no exime a las unidades administrativas de la Comisión a cumplir con las obligaciones previstas en la Ley General.

En caso de considerarse necesario, la Comisión podrá abstenerse de celebrar contratos con Instituciones que no cuenten con los requisitos mínimos de ley en materia de Protección de Datos Personales.

**Artículo 79.** En toda transferencia de datos personales, los servidores públicos responsables comunicarán el aviso de privacidad respectivo al tercero receptor de las transferencias, debiendo documentar detalladamente dicha comunicación.

**Artículo 80.** Acorde con lo previsto en la Ley General, toda transferencia de datos personales que realicen las unidades administrativas de la CONDUSEF deberá formalizarse mediante la suscripción de un instrumento jurídico que demuestre el alcance de su tratamiento, así como las obligaciones y responsabilidades contraídas por las partes.

La formalización referida no resultará aplicable en los siguientes casos:

I. Cuando la transferencia sea nacional y se realice en virtud del cumplimiento de una disposición legal o del ejercicio de las atribuciones expresamente conferidas.
II. Cuando la transferencia sea internacional y se encuentre prevista en una ley o tratado suscrito y ratificado por México; se realice derivado de una petición de la autoridad extranjera u organismo internacional competente en su carácter de receptor; cuando las facultades entre la CONDUSEF y el responsable receptor sean homólogas; o cuando las finalidades que motivan la transferencia sean análogas o compatibles respecto de aquéllas que dieron origen al tratamiento por parte de la CONDUSEF.

**Artículo 81.** Cuando la comunicación de datos personales se realice fuera del territorio nacional, previo a su transferencia, la CONDUSEF se asegurará que el tercero receptor se obligue a proteger los datos personales conforme a los principios, deberes y obligaciones similares o equiparables a las previstas en la Ley General y demás normatividad mexicana aplicable en la materia, así como a los términos previstos en el aviso de privacidad que le será comunicado por la CONDUSEF.

En todo caso, la CONDUSEF podrá solicitar al INAI opinión respecto de las transferencias internacionales que se le susciten, en términos de lo dispuesto en los Lineamientos.

## De las Sanciones

**Artículo 82.** Serán causas de sanción por incumplimiento de las obligaciones en materia de protección de datos personales, las establecidas en el artículo 763 de la LGPDPPSO:

I. Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCOP;
II. Incumplir los plazos de atención para responder las solicitudes para el ejercicio de los derechos ARCOP 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 Ley;
V. No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos a que se refiere el artículo 27 de la Ley, según sea el caso, y demás disposiciones que resulten aplicables en la materia;
VI. Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables;
VII. Incumplir el deber de confidencialidad;
VIII. No establecer las medidas de seguridad en los términos que establecen los artículos 37, 32 y 33 de la LGPDPPSO;
IX. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad;
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 Ley General;
XIII. No acatar las resoluciones emitidas por el Instituto y los Organismos garantes; y
XIV. Omitir la entrega del informe anual y demás informes a que se refiere el artículo 44, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, o bien, entregar el mismo de manera extemporánea;

# Proceso general para el establecimiento, actualización, monitoreo y revisión de los mecanismos y medidas de seguridad.

**Artículo 83.** El artículo 33, fracción VII de la Ley General establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, el monitoreo y revisión de manera periódica de las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales.

De acuerdo con la fracción VI del artículo 35 de la Ley General, los mecanismos de monitoreo y revisión forman parte del documento de seguridad.

Así, respecto a los mecanismos de monitoreo y revisión de las medidas de seguridad, el artículo 63 de los Lineamientos Generales señala lo siguiente:

> ***"Monitoreo y supervisión periódica de las medidas de seguridad implementadas***
> ***Artículo 63.*** *Con relación al artículo 33, fracción VII de la Ley General, el responsable deberá evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, a fin de verificar el cumplimiento de los objetivos propuestos y, en su caso, implementar mejoras de manera continua.*
>
> *Para cumplir con lo dispuesto en el párrafo anterior del presente artículo, el responsable deberá monitorear continuamente 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 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.*
>
> *Aunado a lo previsto en las fracciones anteriores del presente artículo, el responsable deberá contar con un programa de auditoría, interno y/o externo, para monitorear y revisar la eficacia y eficiencia del sistema de gestión."*

De lo anterior es posible identificar que el monitoreo y revisión de las medidas de seguridad tiene el objetivo de fortalecer, a través de un ciclo de mejora continua, la protección de los datos personales que resguarda este sujeto obligado.

**Mecanismos de Monitoreo**

Para los tratamientos de datos personales de la CONDUSEF se consideran los siguientes tipos de monitoreo:

1) Revisión de cumplimiento de las políticas internas en materia de Protección de Datos Personales.

Para ello, en los casos en los que se realiza o identifica algún cambio en los instrumentos referidos, será necesario:

a. Revisar y, en su caso, actualizar los avisos de privacidad, las funciones y obligaciones del personal y los inventarios de datos personales, según corresponda.
b. Evaluar si hubo cambios en las amenazas, vulnerabilidades o impacto de los riesgos relacionados con las modificaciones a la normativa, para actualizar los análisis de riesgos, análisis de brecha y plan de trabajo.
c. Revisar y, en su caso, adecuar los sistemas de tratamiento para cumplir con los cambios normativos.

2) Revisión del riesgo. Tiene el objetivo de identificar modificaciones a los riesgos identificados en los tratamientos de datos personales, para ello, se implementarán los siguientes monitoreos:

a. Monitoreo del entorno físico. Para la detección continua de amenazas y vulnerabilidades en el entorno físico, se cuenta con:

- Personal de vigilancia en los accesos de las dos torres de la CONDUSEF,
- control de acceso del personal, y visitantes, y
- circuito cerrado de cámaras de vigilancia.

b. Monitoreo del entorno electrónico.
c. Actualización del plan de trabajo.
d. Revisión de avances del plan de trabajo.
e. Actualización tecnológica. Cuando se integren nuevos equipos de cómputo, servidores, aplicaciones o tenga lugar una migración tecnológica, se realizará una actualización del análisis de riesgo, análisis de brecha y plan de trabajo.
f. Vulneraciones a la seguridad de los datos personales. En caso de identificar un incidente de seguridad que involucre datos personales, las áreas encargadas junto con el Comité de Transparencia se coordinarán para decidir sobre las acciones pertinentes para mitigar dicho incidente.

**Mecanismos de supervisión o revisión**

Además del monitoreo continuo de las medidas de seguridad, se requiere realizar una supervisión periódica de las medidas de seguridad, a través de auditorías, las cuales pueden ser internas o externas.

Así, respecto del programa de auditoría mencionado en el último párrafo del artículo 63 de los Lineamientos Generales, se tiene contemplada la realización de una auditoría en materia de protección de datos personales, al menos una vez al año, misma que se puede llevar a cabo por terceros según la disponibilidad presupuestal o bien internamente, conforme lo determine el Comité de Transparencia.

El programa de auditoría será determinado por el Comité de Transparencia.

## Transitorio

**ÚNICO.** - El presente documento entrará en vigor al día hábil siguiente de su publicación en la página de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros.